SpectraLink 8020/8030 Wireless Telephone

Administration Guide

Session Initiation Protocol (SIP)

January 2010 Edition
1725-36038-001
Version H

POLYCOM®

Patent Information

The accompanying product is protected by one or more US and foreign patents and/or pending patent applications held by Polycom, Inc.

Copyright Notice

© 2007 to 2010, Polycom, Inc. All rights reserved. POLYCOM®, the Polycom "Triangles" logo and the names and marks associated with Polycom's products are trademarks and/or service marks of Polycom, Inc. and are registered and/or common law marks in the United States and various other countries. All other trademarks are property of their respective owners. No portion hereof may be reproduced or transmitted in any form or by any means, for any purpose other than the recipient's personal use, without the express written permission of Polycom.

All rights reserved under the International and pan-American copyright Conventions.

No part of this manual, or the software described herein, may be reproduced or transmitted in any form or by any means, or translated into another language or format, in whole or in part, without the express written permission of Polycom, Inc.

Do not remove (or allow any third party to remove) any product identification, copyright or other notices.

Every effort has been made to ensure that the information in this document is accurate. Polycom, Inc. is not responsible for printing or clerical errors. Information in this document is subject to change without notice and does not represent a commitment on the part of Polycom, Inc.

Notice

Polycom, Inc. has prepared this document for use by Polycom personnel and customers. The drawings and specifications contained herein are the property of Polycom and shall be neither reproduced in whole or in part without the prior written approval of Polycom, nor be implied to grant any license to make, use, or sell equipment manufactured in accordance herewith.

Polycom reserves the right to make changes in specifications and other information contained in this document without prior notice, and the reader should in all cases consult Polycom to determine whether any such changes have been made.

NO REPRESENTATION OR OTHER AFFIRMATION OF FACT CONTAINED IN THIS DOCUMENT INCLUDING BUT NOT LIMITED TO STATEMENTS REGARDING CAPACITY, RESPONSE-TIME PERFORMANCE, SUITABILITY FOR USE, OR PERFORMANCE OF PRODUCTS DESCRIBED HEREIN SHALL BE DEEMED TO BE A WARRANTY BY POLYCOM FOR ANY PURPOSE, OR GIVE RISE TO ANY LIABILITY OF POLYCOM WHATSOEVER.

Contact Information

Please contact your Polycom Authorized Reseller for assistance.

Polycom, Inc.
4750 Willow Road,
Pleasanton, CA 94588
http://www.polycom.com

About this Guide

This document explains how to configure and maintain the SpectraLink 8020/8030 Wireless Telephones using Session Initiation Protocol (SIP).

Polycom Model Numbers

This document covers the following registered model numbers:

802X, 803X

Related Documents

SpectraLink 8020/8030 Wireless Telephone and Accessories User Guide for SIP (1725-36165-001)

SpectraLink 8000 SVP Server: Administration Guide for SIP (1725-36033-001)

SpectraLink 8020/8030 Wireless Telephone: SIP User Agent: Features and Standards (1725-36037-001)

SpectraLink 8020/8030 Wireless Telephones Handset Administration Tool (7125-36039-001)

Available at http://www.polycom.com/usa/en/support/voice/wi-fi/wi-fi.html

Polycom VIEW Certified Products Guide (1725-36040-001)

VIEW Configuration Guide 1725-36xxx-001 where xxx indicates a number corresponding to the type of access point)

Available at http://www.polycom.com/support/voice/wi-fi/view_certified.html

Deploying Enterprise-Grade Wi-Fi Telephony
Best Practices Guide for Deploying SpectraLink 8020/8030 Wireless Telephones
Available at
http://www.polycom.com/products/voice/wireless_solutions/wifi_communications/handsets/spectralink_8020_wireless.html

Open Application Interface (OAI) Specification (1725-36196-001)
Available at
www.polycom.com/forms/spectralink_oai_sw_dl.html

Asterisk cmd VoiceMailMain (Shows how to enter the Asterisk voicemail system, its menu structure, and related information.)
Available at
http://www.voip-info.org/wiki/index.php?page=Asterisk+cmd+VoiceMailMain

Customer Support

Polycom wants you to have a successful installation. If you have questions, please contact our Customer Support Hotline at (800) 775-5330.

The hotline is open Monday through Friday, 6 a.m. to 6 p.m. Mountain time.

For Technical Support: technicalsupport@polycom.com

For Knowledge Base:
http://www.polycom.com/usa/en/support/voice/voice.html

For Return Material Authorization: rmacoordinator@polycom.com

Icons and Conventions

This manual uses the following icons and conventions.

Caution! Follow these instructions carefully to avoid danger.

Note these instructions carefully.

Label	This typeface indicates a key, label, or button on SpectraLink hardware.

Contents

0 About this Guide 3

Polycom Model Numbers 3
Related Documents 3
Customer Support 4
Icons and Conventions 4

1 SpectraLink 8020/8030 Wireless Telephone Overview 11

WLAN Quality of Service 11
WLAN Security 12
System Diagram 14
System Components 15
SpectraLink 8020/8030 Wireless Telephone Specifications 18
Notes on Battery Packs 20
Startup Sequence 21
Handset Modes 22

2 SpectraLink 8020/8030 Wireless Telephone Configuration 25

The Admin Menu 25
Admin menu 28
Phone Config 32
Network Config 36
Diagnostics 43
Restore Defaults 44
Demos 44

Admin Menu Default Table....45
User-Defined Preferences....47
WPA2 Enterprise PEAP Certificate Enrollment and EAP-FAST Manual PAC Provisioning....50

3 Software License and Protocol Management....55
Minimum System Requirements....55
Minimum Configuration Process....57

4 SIP Integration Factors....59
Sample DHCP Server Configuration File....60

5 Programming the SIP Handset Features....63
SIP TFTP Server Configuration Files....63
Proxy server commands....65
Sample SIP Configuration Files....70

6 Using the SIP Handset....85
The Handset Display....85
Menus....89
Handset Operation....91

7 Testing a Handset....101

8 Diagnostic Tools....103
Run Site Survey....103
Diagnostics Enabled....107
Syslog Mode....112

9 Certifying the Handsets....117
Conducting a Site Survey....117

10 Software Maintenance 121

Upgrading Handsets 121

Normal Download Messages 122

Download Failure or Recovery Messages 122

11 Troubleshooting 123

Access Point Problems 123

Handset Status Messages 125

12 Appendix A: Regulatory Domains 135

13 Index 137

1

SpectraLink 8020/8030 Wireless Telephone Overview

The SpectraLink 8020/8030 Wireless Telephones is a Wi-Fi handset for workplace telephone systems. The handsets operate over a VIEW Certified 802.11a/b/g/n wireless LAN (WLAN) providing users a wireless extension of the SIP call server. By seamlessly integrating into a SIP environment, wireless telephone users are provided with high-quality mobile voice communications throughout the workplace, giving users the freedom to roam throughout the workplace while providing all the features and functionality of a wired SIP desk phone.

In the SIP environment, the handsets support up to three SIP call servers. Each handset may have five line appearances and two calls per line. Each handset may have up to 10 sets of credentials to identify itself by current user.

The latest wireless telephone and Handset Administration Tool software versions are required to support the features described in this document. See Chapter 3 *Software License and Protocol Management.*

WLAN Quality of Service

WLAN Quality of Service (QoS) is provided by using one of three available mechanisms: SpectraLink Voice Priority (SVP), Wi-Fi Standard QoS, or Cisco Compatible Extensions (CCX) version 4. These QoS modes can not be mixed within the same WLAN; therefore, all Wireless Telephones on the network must have the same QoS setting.

SVP

SpectraLink Voice Priority (SVP) is a proprietary method of WLAN QoS, developed by Polycom, to ensure enterprise-grade voice quality, battery life and call capacity for SpectraLink Wireless Telephones.

SVP requires the use of the SVP Server, which is an Ethernet LAN device that works with in conjunction with Wi-Fi APs to ensure QoS over the WLAN. Voice packets to and from the Wireless Telephones are tunneled through the SVP Server to ensure voice prioritization as they are routed between the handset and SIP call server. See the *SpectraLink SVP Server: Administration Guide within IP Environments* document for detailed information about this device.

Wi-Fi Standard QoS

SpectraLink Wireless Telephones support WMM, WMM Power Save and WMM Admission Control - all QoS standards from the Wi-Fi Alliance based on IEEE 802.11e. The combination of these three standards provides enterprise-class QoS in terms of voice quality, battery life and call capacity. The WLAN must also support and enable each of these QoS mechanisms in order to ensure they are utilized. This option does not require the SVP Server.

CCXv4

The CCX program requires WLAN client devices operating on Cisco APs to use a defined set of industry standards and Cisco-specific features. The SpectraLink 8020/8030 Wireless Telephone has been certified by Cisco as CCXv4 compliant. When the CCXv4 operating mode is selected on the handset, it automatically initiates the required set of Cisco-specific and industry standard QoS mechanisms. This option does not require the SVP Server.

WLAN Security

The following security methods are supported by the handset.

WPA2 Enterprise

The handset supports WPA2 Enterprise, as defined by the Wi-Fi Alliance. WPA2, which is based on the 802.11i standard, provides government-grade security by implementing the Advanced Encryption Standard (AES) encryption algorithm. The Enterprise version of WPA2 uses 802.1X authentication, which is a port-based network access control mechanism using dynamic encryption keys to protect data privacy. Two 802.1X authentication methods are supported on the Wireless Telephone, EAP-FAST and

PEAPv0/MSCHAPv2. Both of these methods require a RADIUS authentication server to be available on the network and accessible to the phone. Additional details are provided in Section 3.1.

Normal 802.1X authentication requires the client to renegotiate its key with the authentication server on every AP handoff, which is a time-consuming process that negatively affects time-sensitive applications such as voice. Fast AP handoff methods allow for the part of the key derived from the server to be cached in the wireless network, thereby shortening the time to renegotiate a secure handoff. The Wireless Telephone supports two fast AP handoff techniques, Cisco Client Key Management (CCKM) (only available on Cisco APs) or Opportunistic Key Caching (OKC). One of these methods must be configured for support on the WLAN to ensure proper performance of the handset.

WPA and WPA2 Personal

The handset supports WPA and WPA2 Personal, as defined by the Wi-Fi Alliance. WPA2, which is based on the 802.11i standard, provides government-grade security by implementing the Advanced Encryption Standard (AES) encryption algorithm. WPA, which is based on a draft version of the 802.11i standard before it was ratified, uses Temporal Key Integrity Protocol (TKIP) encryption. The Personal version uses an authentication technique called WPA2 is based on the 802.11i standard. Pre-Shared Key (PSK) allows the use of manually entered keys or passwords to initiate WPA security.

Cisco Fast Secure Roaming

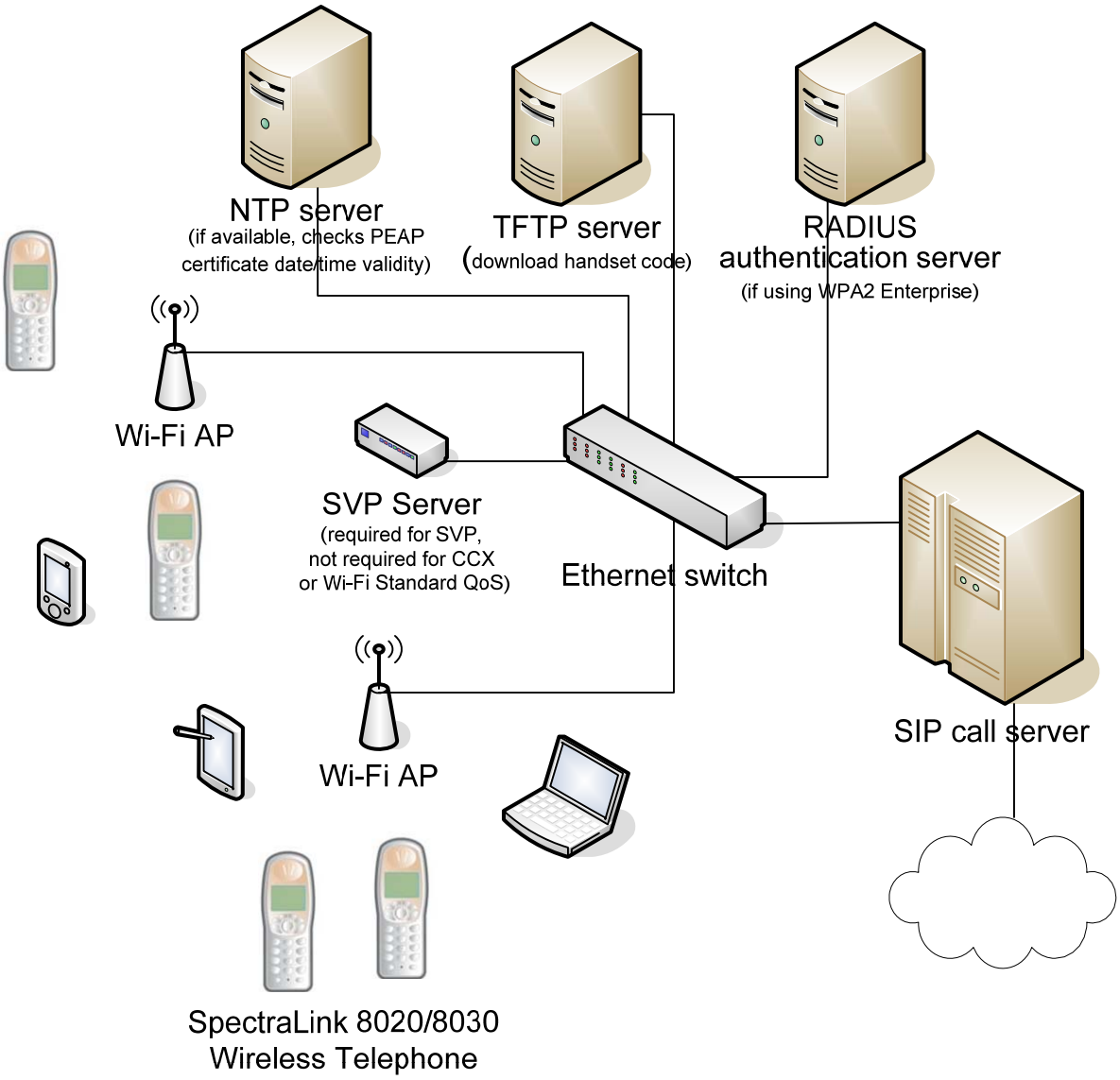
Cisco's Fast Secure Roaming (FSR) mechanism uses a combination of standards-based and proprietary security components including Cisco Client Key Management (CCKM), LEAP authentication, Michael message integrity check (MIC) and Temporal Key Integrity Protocol (TKIP). FSR provides strong security measures for authentication, privacy and data integrity along with fast AP handoff on Cisco APs.

WEP

The handset supports Wired Equivalent Privacy (WEP) with both 40-bit and 128-bit encryption.

System Diagram

The following diagram shows the Polycom components residing on a network with APs and wireless LAN Ethernet Switch.



System Components

SpectraLink 8020/8030 Wireless Telephone

The SpectraLink 8020 Wireless Telephone is a lightweight, durable handset specifically designed for mobile workplace use. The SpectraLink 8030 Wireless Telephone has the same features and function, but in a more durable design with and includes push-to-talk capability.

Like a wired desk phone, the handset can receive calls directly, receive transferred calls, transfer calls to other extensions, and make outside and long distance calls. The Wireless Telephones can only be used on-premises within the WLAN coverage area with the local SIP call server.

SpectraLink 8000 SVP Server (required when using SVP)

As described earlier, the SVP Server is a Polycom wired LAN device that is required when using SpectraLink Voice Priority for QoS.

Access points

Enterprise-grade Wi-Fi access points provide the connection between the wired LAN and the wireless LAN. VIEW Certified 802.11a/b/g/n APs must be positioned in all areas where Wireless Telephones will be used to ensure seamless radio coverage. The number, type and placement of access points will affect the coverage area and capacity of the wireless system. Careful planning of the WLAN is necessary to ensure good voice quality. See the *Best Practices Guide for Deploying SpectraLink 8020/8030 Wireless Telephones* for additional guidance.

APs must be properly configured to support the corresponding QoS and security methods selected for the handset.

Ethernet switch

One or more Ethernet switches interconnect multiple network devices, including the SpectraLink 8000 SVP Server (if used for QoS), the proxy server(s), wired IP phones, TFTP Server, RADIUS authentication server (if using WPA2 Enterprise) and WLAN access points. Enterprise Ethernet switches provide the highest performance

networks, which can handle combined voice and data traffic, and are required when using the SpectraLink 8020/8030 Wireless Telephones.

Although a single Ethernet switch network is recommended, the handsets and the SpectraLink 8000 SVP Server can operate in larger, more complex networks, including networks with multiple Ethernet switches, routers, VLANs and/or multiple subnets, as long as the SVP Server and access points and handsets are on the same subnet. However, in such networks, it is possible for the quality of service (QoS) features of the SVP Server to be compromised, and consequently voice quality may suffer. Any network that consists of more than a single Ethernet switch should be thoroughly tested to ensure any quality issues are addressed. See the *Best Practices Guide for Deploying SpectraLink 8020/8030 Wireless Telephones* for additional guidance.

SpectraLink 8020/8030 Wireless Telephones cannot roam with uninterrupted service between subnets unless specific LAN components are present. Certain AP/Ethernet switch combinations establish a Layer-2 tunnel across subnets that enable the handsets to roam. Without this capability, any call in progress will be dropped when the user moves out of range and the handset must be power cycled in order to resume functionality in the new subnet area.

Ensure that all your APs are attached to the same subnet for proper operation. The handset can change subnets if DHCP is enabled and the handset is powered off then back on when within range of APs on the new subnet. Note that the wireless telephones cannot "roam" across subnets, since they cannot change IP addresses while operational.

SIP server

The SIP server is a component from a third-party vendor that provides access to telephony services. The handsets can recognize up to three distinct SIP servers in a single system.

The handsets can operate with SIP proxy servers such as SER (SIP Extensible Router) or with SIP Back-to-Back User Agents (B2BUA) – the most common form of SIP server for PBX-based systems. In this case the IP address location services provided by the SIP server are not available, so direct IP address dialing must be used.

The SIP proxy server connects to another device such as a PBX or gateway and from there, other wired phones and the PSTN.

TFTP (Trivial File Transfer Protocol) server

A TFTP server is required in the system to distribute software to the handsets. It may be on a different subnet than the APs and/or handsets.

SIP TFTP server

The SIP TFTP server is required in the system to deliver SIP configuration parameters to the SIP handset whenever a SIP handset is powered-up. The location of the SIP TFTP server is separately specified in SIP handset administration parameters (See Chapter 2 *SpectraLink 8020/8030 Wireless Telephone Configuration*, section *The Admin Menu*.) Normally, the SIP TFTP server is the same as the network TFTP server, see above.

NTP (Network Time Protocol) Server

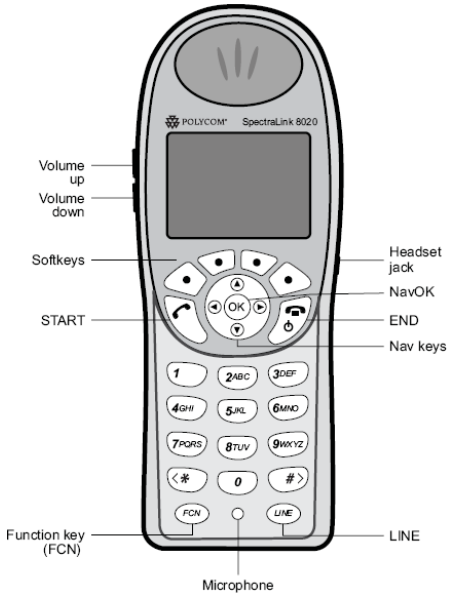
If WPA2 Enterprise security is used, the handset will confirm the PEAP certificate has a valid date and time with the NTP Server on the network, if one is available. If an NTP Server is not available, the certificate will be assumed valid and operate accordingly.

Authentication Server (if using WPA2 Enterprise)

A RADIUS authentication server must be used to provide username/password-based authentication using RSA certificates for PEAPv0/MSCHAPv2 or PAC files for EAP-FAST.

SpectraLink 8020/8030 Wireless Telephone Specifications

SpectraLink 8030 Wireless Telephone



SpectraLink 8020 Wireless Telephone

Table of Specifications

Radio mode (selectable)	(802.11b, 802.11g)	2.4–2.4835 GHz
	(802.11a)	5.150–5.250 GHz 5.250–5.350 GHz 5.470–5.725 GHz 5.725–5.825 GHz
Transmission type	Direct-sequence spread spectrum (DSSS)	
Transmit data rate	up to 54 Mb/s	
WLAN QoS	SpectraLink Voice Priority (SVP) Wi-Fi Standard QoS (using WMM, WMM-Power Save and WMM-Admission Control) CCXv4	
WLAN security	WEP (Wired Equivalent Privacy) Cisco FSR (Fast Secure Roaming) WPA Personal WPA2 Personal WPA2 Enterprise: 802.1X Authentication EAP-FAST PEAPv0/MSCHAPv2: PEAP certificate sizes: 512*, 1024*, 2048, 4096 bit (*recommended) Encryption Ciphers: AES, RSA, RC4 Data Integrity: Hashed Message Authentication Code MD5 (HMAC-MD5) (RFC 2403, 2104) and Secure Hash Algorithm-1 SHA (HMAC-SHA-1) (RFC2404) Fast AP Handoff Opportunistic Key Caching (OKC) Cisco Client Key Management (CCKM)	
FCC certification	Part 15.247	
Other certifications	IP 53 certified for resistance to dust and liquid resistance MIL 810F Proc IV 516.5 for shock resistance Cisco Compatible Extensions (CCX) v4	
Voice encoding	ADPCM (Proprietary) G.711µ-law, G.711a-law and G.729	
Transmit power	Up to 100mW Transmit Power Control (formerly 802.11h), see Appendix A for details.	
Display	Up to five lines of text plus two icon status rows and one row for softkey labels.	
8020 Dimensions	5.7" x 2.0" x 0.9" (14.5 x 5.1 x 2.3 cm)	

8030 Dimensions	5.4" x 2.0" x 0.9" (13.7 x 5.1 x 2.3 cm)
8020 Weight*	3.9 oz. (110.6 g) with Standard Battery Pack
8030 Weight*	4.2 oz. (119.1 g) with Standard Battery Pack
Standard Battery Pack capacity	4 hours talk, 80 hours standby
Extended Battery Pack capacity	6 hours talk, 120 hours standby
Ultra-Extended Battery Pack capacity	8 hours talk, 160 hours standby

Notes on Battery Packs

- Polycom offers the following battery types with increasing capacity: Standard, Extended and Ultra-Extended.
- Battery Pack life will vary depending on handset model and features and system infrastructure.
- Batteries are shipped with a partial charge. Polycom recommends fully charging them before using them in phone operation.
- Maximum Battery Pack performance is achieved after a few charge/discharge cycles.
- If multiple Battery Packs are supplied with your handset, Polycom recommends that each be fully charged upon receipt to prolong battery life. Battery Packs will slowly lose charge if unused. To maintain battery potential, charge unused Battery Packs occasionally or alternate Battery Pack use.
- After a length of time Battery Packs will lose the ability to maintain a charge and to perform at maximum capacity and will need to be replaced. This is normal for all batteries.
- Overnight charging is best done while the handset is turned off.
- If the handset does not charge, clean Battery Pack, charger and handset contacts with an alcohol swab.
- When the handset is properly seated, the backlight comes on briefly to indicate charging has begun.
- Any battery which exhibits swelling, cracking or other abnormality should be disposed of promptly and properly.

Startup Sequence

The SpectraLink 8020/8030 Wireless Telephone goes through an initialization sequence at startup. The line icons 1-9 display and count down as the handset steps through this sequence. This is usually very rapid. If there is difficulty at any step that prevents initialization from continuing, an error message will display and the related icon(s) will stay on. Please see the error table at the back of this document for instructions on how to handle error messages that occur during initialization.

Icon	The icon(s) shown in bold turns off when:
123456789	The handset has located and authenticated and associated with at least one AP, and is proceeding to bring up higher-layer networking functions.
12345678	The handset is either configured for Static IP, or if configured for DHCP, the DHCP discovery process has started.
1234567	If DHCP is configured, a DHCP response was received which contains a good DNS server configuration.
12345**6**	Note: Used for SVP QoS only and not present when using Wi-Fi Standard QoS or CCXv4. Indicates one of the following possibilities: 1. Static IP configuration 2. SVP Server address found in DHCP option 151 response 3. SVP Server address found via DNS lookup
1234**5**	All networking functions are complete (notably, DHCP), and the handset is proceeding with establishing the SRP link to the SpectraLink 8000 SVP Server.
123**4**	Note: Used for SVP QoS only and not present when using Wi-Fi Standard QoS or CCXv4. The SRP link is established; all network stack initialization is complete, proceeding with application-specific initialization.
12**3**	SIP application startup. Icon 3 is extinguished if a generic SIP config file is found.
1**2**	Icon 2 is extinguished if a handset specific SIP config file is found.
(no icons) **Registering**	Handset is attempting to register each of the specified line contacts.

Icon	The icon(s) shown in bold turns off when:
(no icons) **EXT. XXXXX**	Handset has registered with at least one contact on one proxy server. Initialization is complete. The handset is in standby mode ready to receive and place calls. The line one contact is displayed.

During the last three steps of this process, the handset contacts the SIP TFTP server and downloads general information about the proxy server(s), downloads specific information pertaining to the handset, registers with the proxy server(s), and verifies handset credentials. Once this process is complete, the handset is ready to use.

If the username and password have not been defined in the **Admin** menu, you will be prompted to enter both of these items before the extension number can display. The user name must correspond to the configuration file that contains user-specific information. If the file is not found, an error message will appear and the handset will restart. See Chapter 5 *Programming the SIP Handset Features*, section *SIP TFTP Server Configuration Files*.

Handset Modes

Standby mode (on-hook)

In standby mode, the handset is waiting for an incoming call or for the user to place an outgoing call. The extension number is shown on the display and there is no dial tone. In this mode, the handset is conserving battery power and wireless LAN bandwidth.

When an incoming call arrives, the handset rings; the handset enters the active mode and remains so until the call is ended. The call is answered by pressing the **START** key or the **Answ** or **Spkr** softkey. The handset will ring according to user preference as specified in the standby menus. The ringing can be silenced by pressing the **END** key. If you do not wish to accept the call, some SIP call servers support the ability to press the **Rej** softkey. If supported, the SIP call server will redirect the call as configured by the system administrator.

Active mode (off-hook)

The handset is in the active mode when an incoming call is answered or when it is in communication with the SIP server without being in an active call.

When an incoming call occurs during an active call, the handset will play the second call ringing sound until the call is answered, the caller hangs up, or the call transfers to voicemail. If the **END** key is pressed, the first call is terminated and the handset reverts to a full ring.

The active mode utilizes the most bandwidth and battery power. To conserve battery resources, return the handset to the standby mode when a call is completed by pressing the **END** key.

Push-to-talk (PTT) mode

The SpectraLink 8030 Wireless Telephones utilize channels for incoming and outgoing radio communication. While PTT is active, the handset is in PTT mode. It can receive regular phone calls in this mode. When a regular phone call is answered, the handset enters active mode.

Configuration menu mode

When user preferences are being configured in the Config menu, the handset is on but is not active. It cannot receive calls while in the Config menu. If the handset is idle 15 seconds while in the Config menu, it will return to the standby state. If a call was trying to be established while in the Config menu, it will ring as soon as it is returned to the standby state.

Messaging mode

If text messaging functions have been programmed, as in a nurse call system, the handset is able to receive text messages. While these messages are being accessed, the handset is in messaging mode. Incoming calls will ring with the second call ringing sound.

2

SpectraLink 8020/8030 Wireless Telephone Configuration

Each handset may be configured for site-specific requirements by opening the **Admin** menu and selecting options or entering specific information. Any settings entered in the **Admin** menu must conform to system settings. Only the handset being configured is affected by the **Admin** menu settings.

The wireless telephone user may select several usability options from the Standby menu, described below in the *User-defined Preferences* section. This information is also provided in the end-user manual.

The SpectraLink Handset Administration Tool is a software utility that enables rapid configuration of handsets by utilizing the USB port on the Dual Charger. See the *Handset Administration Tool (HAT)* document for specific instructions. Please see your service representative or contact Polycom customer service for more information about this time-saving tool.

When WPA2 Enterprise security is used, PAC files for EAP-FAST can be provisioned wirelessly or by using the HAT. For PEAP, the HAT must be used to enroll certificates. See section *WPA2 Enterprise PEAP Certification Enrollment and EAP-FAST Manual PAC Provisioning* at the end of this chapter for details.

Other settings that must be configured include, but are not limited to, WLAN QoS, DSCP tagging, DHCP and regulatory domain information. If these are not selected by the administrator the handset will use the default settings.

The Admin Menu

The **Admin** menu contains configuration options that are stored locally (on each handset). Each handset is independent, and if the default settings are not desired, the **Admin** options must be set in each handset requiring different settings.

Opening the Admin menu

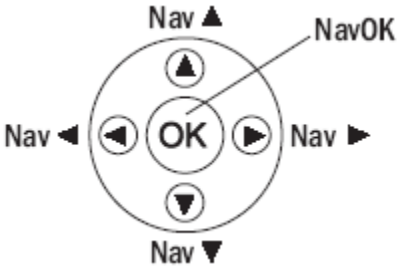
The handset Admin menu can be accessed in one of two ways:

1. With the handset powered off, press and hold the **START** key. While holding the **START** key, press and release the **END** key. When the **Admin** menu appears, release the **START** key.
2. Press and release the **END** key. Press and hold the **START** key. When the **Admin** menu appears, release the **START** key.

If an admin password has been set, the display will require its entry before opening the **Admin** menu. The default password is 123456. If no password is set, the display will proceed directly into the **Admin** menu.

Navigation

The navigation keys just below the softkeys are used to navigate through and select menu options. These are referred to as **Nav▲**, **Nav▼**, **Nav◄**, **Nav►**, and **NavOK**.



Toggle options

Some menu items have only two options, which operate on a toggle basis. The current setting is shown below the menu heading on the info line. The other available setting is highlighted in the menu list. Press **NavOK** to activate the highlighted setting.

For example, when predial is disabled, the info line displays **Predial Disabled** and the highlighted menu item is the **Enable Predial** option. Press **NavOK** to enable predial. The info line will change to display **Predial Enabled**.

In another example, when the info line displays **Ring in Speaker**, the highlighted menu option is **Ring in Headset**. Press **NavOK** to select **Ring**

in Headset, The ring will now sound in the headset and the info line will change to **Ring in Headset**.

Data entry and editing

An asterisk (*) next to an option on the display indicates that it is selected. Use the **Nav** keys and the softkeys to navigate and select desired options.

Enter numbers by pressing the buttons on the keypad. The blinking underscore identifies the current cursor position. When entering alphanumeric strings, the **CAPS**/**caps** softkey will appear and may be pressed to toggle the case. Enter letters by repeatedly pressing the corresponding key until the desired letter displays on the screen. Use the **CAPS** softkey to change the case as needed.

To edit during entry, delete the character to the left of the cursor by pressing the **Del** softkey. To replace an entry, delete it by pressing the **Clr** softkey and then enter the new data. To edit an existing entry, use **Nav◄** and **Nav►** to move the cursor position, and then press the **Del** softkey to delete the character to the left. Insert new data by pressing the buttons on the keypad.

Alphanumeric entries:

Key	caps	CAPS
1	1	1
2	2 a b c	2 A B C
3	3 d e f	3 D E F
4	4 g h I	4 G H I
5	5 j k l	5 J K L
6	6 m n o	6 M N O
7	7 p q r s	7 P Q R S
8	8 t u v	8 T U V
9	9 w x y z	9 W X Y Z
0	0	0
*	* . ! $ % & ’ ( ) + , : ; / \ = @ ~	
#	<space>	

Admin menu

The following table lists the **Admin** menu items. The default settings have an * prior to the option. Detailed descriptions of each item appear below the table.

1st level	2nd level	3rd level	4th level	5th level
Phone Config	Telephony Protocol	*Type 036		
	PTT/Emerg. Button	Emergency Dial	Emergency # [Enable/Disable]	
			Emergency Number	[Enter Number] [Enter Name]
		PTT	PTT [Enable/*Disable]	
			Allowed Channels	*Channel 1 *Channel 2 *…. *Channel 24
			Name Channels	[list]
			Priority Channel	Priority Channel On/*Off
				Name Channel
	Time Zone	[list] *GMT		
	Daylight Savings	*DST No Adjust DST Auto (USA) DST Auto (AUS) DST Auto (EURO)		
	Password *Enable/Disable			
	[If Password is enabled] Change Password			
	SIP Registration	Login Reg 2 Reg 3 Reg 4	[for each option] Username Password	
	Clear SIP Regist.			
	OAI	*Enable OAI		

1st level	2nd level	3rd level	4th level	5th level
		Disable OAI		
	Location Service	Enable RTLS *Disable RTLS		
		Transmit Interval	1 minute 5 minutes *10 minutes	
		Location Server IP	Enter IP	
		ELP Port	Enter Port *8552	
Network Config	IP Addresses	*Use DHCP		
		Static IP	Phone IP Default Gateway Subnet Mask TFTP Server IP Syslog Server IP Time Server IP SVP Server IP SIP TFTP Svr IP OAI Server IP	
	SS ID	[enter]		
	WLAN Settings			

3rd level	4th level	5th level	6th level	7th level
*Custom	Security	*None		
		WEP	Authentication	*Open System Shared Key
			WEP [Enable/*Disable]	
			Key Information	Default Key Key Length Key 1-4
			Rotation Secret	
		WPA2-PSK	*Passphrase Pre-Shared Key	
		WPA-PSK	*Passphrase Pre-Shared Key	
		Cisco FSR	Username Password	

3rd level	4th level	5th level	6th level	7th level
		WPA2-Enterprise	Authentication	*EAP-FAST PEAP
			Fast Handoff	*CCKM OKC
			Username	
			Password	
			Delete [Cert./PAC]	
	QoS	*SVP	DSCP tags	WT in call (*46) WT standby (*26) Other (*0)
		Wi-Fi Standard	DSCP tags	Voice (*46) Control (*26) Other (*0)
			Admission Cntrl	*Mandatory Optional
CCX	WPA2-Enterprise	Authentication	*EAP-FAST PEAP	
		Fast Handoff	*CCKM	
		Username		
		Password		
		Delete [Cert./PAC]	[Yes/No]	
	QoS	DSCP tags	Voice (*46)	
			Control (*26)	
			Other (*0)	

1st level	2nd level	3rd level	4th level	5th level
Network Config	Reg. Domain	01		
		02		
		03		
		04		
		05		
		06		
		07		
		08		

1st level	2nd level	3rd level	4th level	5th level
		→	[802.11 Config]	
			a →	[802.11a]†
				5.150–5.250
				5.250–5.350 DFS
				5.470–5.725 DFS
				5.470-5.650 DFS
				5.725–5.825
				5.725-5.850
			‡b & b/g mixed	
			g only	
			→	[Transmit Power]
				5mW (7dBm)
				10mW (10dBm)
				20mW (13dBm)
				*30mW (15dBm)
				40mW (16dBm)
				50mW (17dBm)
				100mW (20dBm)
Diagnostics	Run Site Survey			
	Diagnostics Mode	*Disable		
		Enable		
	Syslog Mode	*Disabled		
		Errors		
		Events		
		Full		
	Error Handling Mode Halt on Error/ *Restart on Error			
Restore Defaults				
Demos	Graphics Demo			

* default setting

† Only those 802.11a bands that are available in the selected domain will be listed. See Appendix A for complete information.

‡ Subbands have not been established for the b and b/g mixed or the g-only mode at this writing. Provision is made in the software to accommodate these ranges once established. Until added, selecting either of these two modes will immediately bring up Transmit Power options.

Attention: Modifications of settings under WLAN Settings = "CCX" may get reflected in the corresponding settings under WLAN Settings = "Custom" or vice versa. If the configuration is changed from "CCX" to "Custom" or vice versa, it is recommended to double-check all settings.

Phone Config

Telephony Protocol

Telephony Protocol lets you select the VoIP protocol that your site is licensed to download and run. The SIP protocol used for the SpectraLink 8020/8030 Wireless Telephones requires license option selection **36**. Any other protocol will cause the handset to malfunction.

PTT/Emerg. Button

This option appears only on the SpectraLink 8030. The Push-to-talk button on the left side of the handset may be configured to either standard PTT functionality or to dial the specified emergency call number when pressed twice within two seconds. These are mutually exclusive options. Both are disabled by default.

When using the Handset Administration Tool to configure this option, ensure the PTT option in the **PTT Admin tab** under **Handset type** is disabled before enabling the **Emergency Dial** option in the **Phone Config** tab. When **PTT** is enabled, the **Emergency Dial** option will be grayed out.

Push-to-talk [Disable/Enable] – If enabled, the PTT options will appear on the **Config** menu for the end user to subscribe to allowed channels, etc. If disabled, the PTT options will not appear on the **Config** menu and the Emergency Dial option may be enabled.

PTT is disabled by default. When enabled, all 24 PTT channels are allowed by default. To toggle the allowed status of any channel, select **Allowed Channels**, scroll to the channel to be disallowed and press **NavOK**. Allowed channels are displayed with an asterisk (*) in the left column. Only those channels allowed in the **Admin** menu will appear on the Config menu where they can be subscribed to by the end user. The priority channel, labeled by default as channel 25, may be set and will be available to all PTT handsets. When a PTT broadcast is made on the priority channel, it will override any active PTT transmission on all other channels.

Emergency Dial – the **Emergency Dial** option allows you to enable or disable the feature. When enabled, the handset will dial the number programmed into the **Emergency Number** option when the panic button is pressed twice within two seconds.

Caution! Emergency dial just sets up a telephone call and will be inoperable if the wireless system or the call server fails for any reason. Do not rely on it as your sole method of emergency notification.

Follow your dial plan rules when entering the emergency number to be dialed. E.g. if an outside number is to be dialed and a prefix is required to obtain an outside line, enter the prefix as part of the emergency number.

Once an Emergency Number has been entered, it can be modified, but can only be cleared by restoring the handset to defaults.

Time Zone

Worldwide time zone options are available. Greenwich Mean Time (GMT) is the default.

Daylight Savings

The handset may be adjusted for daylight savings time.

Password Enable/Disable/Change

The password option controls access to the **Admin** menu. It is enabled by default with the password 123456. The **Password** option operates as a toggle between **Enabled** and **Disabled**. The info line will display the current state. Press **NavOK** to change the password protection state. To modify the password requirement, the default or previously set password must be entered to verify the change. **Change Password** will appear only if the password is enabled. The password is disabled by default. The password must be set in each handset for which controlled access is desired.

SIP Registration

Individual handsets may be configured to correspond with the SIP configuration information in the TFTP server. The handset is then

automatically identified at startup. If username and password information is not configured in the **Admin** menu, then this information will be requested at startup

In either case, the username must agree with a corresponding configuration file. See Chapter 5 *Programming the SIP Handset Features*, section *SIP TFTP Server Configuration Files*.

Login allows you to specify a username and password for automatically acquiring SIP configuration information. If no username is specified, the SIP handset will request username and password at startup and any additional registrations specified here are ignored.

The username should correspond to the primary (line 1) dial number assigned to the user. The username and password should also correspond to the authentication credentials as created by your system administrator for your primary line registration. Usernames or passwords can be erased by selecting the item, then pressing the **Bksp** softkey and then the **Save** softkey.

Reg 2, **Reg 3**, and **Reg 4** allow you to specify additional authentication usernames and passwords that may be required by your handset for any additional line appearances (registrations) that may appear in the specific user's configuration file. This information will be ignored if a **Login** username is not provided.

OAI Enable/Disable

Polycom's Open Application Interface (OAI) enables third-party computer applications to display alphanumeric messages on the handset display and take input from the handset keypad. Refer to the *OAI Specification (Version 2.0)* documentation for information about administering the OAI Gateway and the services it can provide.

If you have an OAI Gateway installed in your system, OAI may be optionally enabled in each handset. You may select whether the handset should attempt to connect to the SpectraLink 8000 OAI Gateway by choosing either the **Enable** or **Disable** options in this menu.

If OAI is enabled, and an IP address (called the **OAI Server IP**) is available to the handset (either via DHCP or Static IP configuration), the handset will communicate with the OAI Gateway at power-on, and periodically while it is powered-on. If you don't have a SpectraLink 8000 OAI Gateway installed at your site, you should disable the OAI feature to preserve network bandwidth and battery life.

Location Service

Location service may be used to enable or disable the Ekahau Real-Time Location System (RTLS), select a transmit interval, or enter a static IP address for the Ekahau Positioning Engine (EPE). Location services capability is provided by the EPE 4.0 using Ekahau Location Protocol (ELP). See Ekahau's user documentation for more information.

RTLS [Enable/Disable] The RTLS is disabled by default. Press **NavOK** to toggle to the alternate setting. When RTLS is enabled, the handset will display the RTLS icon in the top center of the screen.

The ring indicator icon will take precedence over the RTLS icon, i.e. the new icon will not be visible while the handset is ringing. When ringing has ceased and the ring indicator becomes inactive, the RTLS icon will again appear (regardless of hook state).

Transmit interval Allows selection of **1 minute**, **5 minutes**, or **10 minutes** for maximum time between transmit intervals. Default transmit interval is 10 minutes. Press **NavOK** to select the desired transmit interval.

To optimize battery life, the interval between sending out ELP updates will vary based on handset state. It is expected that ELP updates will occur at most every two to six seconds and at least every few minutes. If improved tracking capability is desired, set the transmit interval for a shorter time between ELP updates. Increasing the frequency of transmissions will decrease battery life.

Location Server IP Allows the user to statically enter the IP address of the EPE. Enter the IP address and press **NavOK** to save.

Ekahau clients are not expected to find the EPE automatically. Regardless of the handset's selection of DHCP or static IP, the EPE IP address must be statically entered in the Ekahau admin menus or HAT.

ELP Port Allows the user to select the port number which ELP updates get sent to at the Location Server IP address. It must match the value configured in the Ekahau Positioning Engine for proper functionality. The ELP port number must be greater than zero and less than 65536. Default is 8552. Enter the port number and press **NavOK** to save.

Network Config

IP Addresses

There are two modes in which the handset can operate: DHCP-enabled or Static IP. Select the mode for operation from the IP Address menu:

*** Use DHCP** Will use Dynamic Host Configuration Protocol to assign an IP Address each time the handset is turned on. If DHCP is enabled, the handset also receives all other IP Address configurations from the DHCP server.

Static IP Allows you to manually set a fixed IP Address. If selected, the handset will prompt for the IP addresses for each configurable network component. When entering addresses, enter the digits only, including leading zeroes. No periods are required.

Regardless of the mode in which the handset is operating, the following components are required and must be configured as part of the SIP system:

Phone IP The IP address of the handset. This is automatically assigned if DHCP is used. If using Static IP configuration, you must obtain a unique IP address for each handset from your network administrator.

Default Gateway and Subnet Mask Used to identify subnets, when using a complex network, which includes routers. Both of these must be configured either with an IP address under Static IP (not set to 000.000.000.000 or 255.255.255.255) or with DHCP for the handset to contact any network components on a different subnet. If configured on the DHCP server, use option 3 for the Default Gateway and option 1 for the Subnet Mask. Contact the network administrator for the proper settings for the network.

SpectraLink 8020/8030 Wireless Telephones cannot roam with uninterrupted service between subnets unless specific LAN components are present. Certain AP/Ethernet switch combinations establish a Layer-2 tunnel across subnets that enable the handsets to roam. Without this capability, any call in progress will be dropped when the user moves out of range and the handset must be power cycled in order to resume functionality in the new subnet area.

Ensure that all your APs are attached to the same subnet for proper operation. The handset can change subnets if DHCP is enabled and the handset is powered off then back on when within range of APs on the new subnet. Note that the wireless telephones cannot "roam" across subnets, since they cannot change IP addresses while operational.

Please see *Best Practices for Deploying Enterprise-Grade Wi-Fi Telephony* for detailed configuration information.

TFTP Server IP The IP address of a TFTP server on your network, which holds software images for updating the handsets and contains the handset files. If this feature is configured (not set to 0.0.0.0 or 255.255.255.255) with either Static IP configuration or using DHCP option 66 (TFTP server), or the boot server/next server (siaddr) field, the handset will check for newer software each time it is powered on or comes back into range of your network. This check takes only a second and ensures that all handsets in your network are kept up-to-date with the same version of software.

Syslog Server IP The IP address of the syslog server. See the *Diagnostic Tools* section for more information.

Time Server IP The IP address of the time server.

SVP Server IP The IP address of the SpectraLink 8000 SVP Server. If using Static IP configuration, this is simply the IP address of the SpectraLink 8000 SVP Server. Note that the SpectraLink 8000 SVP Server must be statically configured to have a permanent IP address. If DHCP is being used, the handset will try the following, in order: the DHCP option 151, then a DNS lookup of "SLNKSVP2" if the DHCP options 6 (DNS server) and 15 (Domain Name) are configured.

SIP TFTP Server IP The IP address of a TFTP server on your network, which holds SIP configuration files. In static mode, this parameter must be configured with an IP address. In DHCP mode, the SIP TFTP server may be specified by defining the address on the DNS

server for the name "siptftp" If this is not defined, the address specified in option 66 or the boot server/next server (siaddr) field will be used. See Chapter 4, *SIP Integration Factors*.

OAI Server IP The IP address of the SpectraLink 8000 OAI Gateway. If using Static IP configuration, this is simply the IP address of the SpectraLink 8000 OAI Gateway. If DHCP is being used, the handset will try the DHCP option 152.

SSID

Enter the SSID.

WLAN Settings

Select between Custom and CCX modes. The Custom mode allows explicit control of all of the security and QoS settings. Using CCX mode automatically enables the CCXv4 features and functions, with only the 802.1X mechanism needing to be selected.

Custom – Security

Handset security setting should match exactly the settings in your APs. Consult the *VIEW Configuration Guide* for the APs installed in your facility for information on which of the security methods are certified.

Encryption keys, Username and Password display as they are entered. For security reasons, these items will not display when a user returns to the Administration menu.

***NONE** disables any 802.11 encryption or security authentication mechanisms.

WEP (Wired Equivalent Privacy) is a wireless encryption protocol that encrypts data frames on the wireless medium allowing for greater security in the wireless network. If WEP is required at this site, you must configure each handset to correspond with the encryption protocol set up in the APs. Select the entries from the options below to enable the handset to acquire the system.

Authentication
Select either **Open System** or **Shared Key**.

WEP Enable/Disable
Select either **Enable WEP** or **Disable WEP**.

Key Information

Default Key Enter the key number specified for use by the handsets. This will be **1** through **4**.

Key Length Select either **40-bit** or **128-bit** depending on the key length specified for use at this location.

Key 1-4 Scroll to the key option that corresponds to the **Default Key** that was entered above. Enter the encryption key as a sequence of hexadecimal characters. (Use the **2** and **3** keys to access hexadecimal digits A through F.

Rotation Secret

This is used for proprietary WEP key rotation. Refer to your custom document if this feature is supported in your system.

Cisco FSR (Fast Secure Roaming) FSR is designed to minimize call interruptions for SpectraLink 8020/8030 Wireless Telephone users as they roam throughout a facility. Cisco FSR requires specific configuration of the Cisco APs in your site. See your Cisco representative for detailed documentation on configuring the APs and other required security services on the wired network. To configure Cisco FSR on a handset, you must enter a Radius Server username and password into each handset.

Username

Enter a username that matches an entry on the RADIUS server. Usernames are alphanumeric strings, and can be entered using the alphanumeric string entry technique.

Password

Enter the password that corresponds to this Username.

WPA2-Enterprise

The **Authentication** setting can select either ***EAP-FAST** or **PEAP** as the authentication method for RADIUS server such as those from Cisco, Microsoft, or Juniper.

Fast Handoff allows the use of either ***CCKM** or **OKC**. These mechanisms allow a phone to quickly and securely roam between APs with a minimum disruption of audio.

Username: Enter a username that matches an entry on your RADIUS server. Alphanumeric strings can be entered using the alphanumeric string entry technique.

Password: Enter the password that corresponds to this username.

The **Delete [PAC/Cert.]:** option removes expired credentials from the phone. When the authentication method is EAP-FAST the PAC

on the phone is deleted. If the RADIUS server has enabled "anonymous in-band PAC provisioning", then the phone will automatically re-acquire these credentials from the RADIUS server over the air. When the authentication method is PEAP or EAP-FAST manual provisioning, the credential on the phone is deleted and a new one needs to be downloaded through the HAT. See additional details in *WPA2 Enterprise PEAP Certificate Enrollment and EAP-FAST Manual PAC Provisioning* section later in this chapter.

Custom – QoS

SVP mode uses the SVP Server to provide enterprise-grade QoS.

DSCP tags are used to change the priority settings for various classes of packets as they are transmitted to the network from the Wireless Telephone. Default values are given but may be overwritten: **WT in call = 46, WT standby = 26, Other = 0**.

Wi-Fi Standard QoS mode uses standards-based traffic controls for QoS, instead of the SVP Server.

DSCP tags are used to change the priority settings for various classes of packets as they are transmitted to the network from the Wireless Telephone. Default values are given but may be overwritten: **Voice = 46, Control = 26, Other = 0**.

Admission Cntrl is used to enable and disable the use of WMM Admission Control by the handset for the AC_VO and AC_VI access categories. If the WLAN is using WMM Admission Control, the handset should be set to ***Mandatory**. If the WLAN is not using WMM Admission Control, the handset should be set to ***Optional**. See the *Best Practices Guide for Deploying SpectraLink 8020/8030 Wireless Telephones* for a detailed explanation of the use of WMM Admission Control.

CCX

CCX settings configure the handset for operation as a CCX V4 certified client.

WPA2-Enterprise

The **Authentication** setting can select either ***EAP-FAST** or **PEAP** as the authentication method for RADIUS server such as those from Cisco, Microsoft, or Juniper.

Note that for **Fast Handoff**, the only selection available is ***CCKM.**

Username: Enter a username that matches an entry on your RADIUS server. Alphanumeric strings can be entered using the alphanumeric string entry technique.

Password: Enter the password that corresponds to this username.

The **Delete [PAC/Cert.]**: Option removes expired credentials from the phone. When the authentication method is EAP-FAST the PAC on the phone is deleted. If the RADIUS server has enabled "anonymous in-band PAC provisioning", then the phone will automatically re-acquire these credentials from the RADIUS server over the air. When the authentication method is PEAP or EAP-FAST manual provisioning, the credential on the phone is deleted and a new one needs to be downloaded through the HAT. See additional details in *WPA2 Enterprise PEAP Certificate Enrollment and EAP-FAST Manual PAC Provisioning* section later in this chapter.

QoS – DSCP tags are used to change the priority settings for various classes of packets as they are transmitted to the network from the Wireless Telephone. Default values are given but may be overwritten: **Voice = 46, Control = 26, Other = 0**.

Regulatory Domain/802.11 Config/Transmit Power

Regulatory domain, 802.11 configuration and transmit power are interdependent. See *Appendix A: Regulatory Domains* for regulatory domain setting specifications. Polycom recommends that you check with local authorities for the latest status of national regulations for both 2.4 and 5 GHz wireless LANs. A regulatory domain must be selected in order for the handset to operate. There is no default setting.

FCC requirements dictate that the menu for changing the regulatory domain be available by password, which in our case is the **LINE** key. Press **LINE** and then navigate to the desired domain. Press **NavOK** to set the domain.

01 - North America

02 – Europe

03 – Japan

04 – Singapore

05 – Korea

06 – Taiwan

07 – Hong Kong

08 – Mexico, India

802.11 config

Once the regulatory domain is set, the **802.11 Config** modes are displayed. Only one may be chosen. **802.11(b & b/g mixed)** is the default. Press **NavOK** to set the mode. If the mode has subbands, the **Subband** list will open. If the mode does not have subbands, the **Transmit Power** list will open.

Use **g only** mode if all of your infrastructure and client devices will use only 802.11g. The handsets will operate up to 54 Mb/s in this mode. If any 802.11b capable clients or infrastructure are used in your wireless LAN then do not use **g only** mode, instead use **802.11b and b/g mixed** mode for optimum performance.

Use **b & b/g mixed** if some of your infrastructure components only understand 802.11b. The handsets will operate up to 11 Mb/s.

Subbands have not been established for the **b and b/g mixed** or the **g only** mode at this writing. Provisions are made in the software to accommodate these ranges once established. Newly added subbands may not appear in the **Admin** menu table above.

Subband

Once a mode is set the subband list will display, if applicable. Only those ranges which are allowed in the set regulatory domain and that pertain to the set mode are displayed. Note that for 802.11a the bands labeled **DFS** will vary depending on the set regulatory domain. Multiple subbands may be set. Navigate to the desired subband and set with **NavOK.** The **Transmit Power** menu will open. Once the **Transmit Power** setting is done, you will be returned to the subband list.

To deselect a subband, navigate to it and press **NavOK**.

Once the subband settings are as desired, press the **Done** softkey to exit to the **Network Setup** menu.

Transmit power

For subbands: The **Transmit Power** list opens when **NavOK** is pressed from the **Subband** menu. A transmit power setting is required for each subband. Only one level may be set per subband. Only those power levels which apply to the regulatory domain and 802.11 mode are listed. Navigate to the

desired level and press **NavOK** to set and return to the subband list. Another subband may be selected which repeats the process.

If the highlighted power transmit level is legal on all of the subbands for the set mode, an **All** softkey will appear. Press the **All** softkey to apply that level to all subbands and return to the subband menu where all subbands will now be selected. **All** overrides any previously set power transmit levels.

Without subbands: When the 802.11 mode has no subbands, the **Transmit Power** list opens when **NavOK** is pressed to set the mode. Only those power levels which apply to the domain and 802.11 mode are listed. Navigate to the desired level and press **NavOK**. This sets the transmit power level and exits the **Regulatory Domain** menus. The **Network Setup** menu will again display.

Note that the power setting selected specifies the maximum for that band/subband. When Transmit Power Control (TPC) is enabled in the infrastructure, the AP may instruct the handset to use a lower value to match its own transmit power.

Diagnostics

Run Site Survey

The **Site Survey** mode is activated by selecting this option. The site survey starts running immediately upon selecting this option. See the *Diagnostic Tools* section for more information about site survey.

Diagnostics Mode

Diagnostics can be enabled or disabled. See Chapter 8 *Diagnostic Tools*, section *Diagnostics Enabled* for a detailed explanation of the **Diagnostics** mode options.

Syslog Mode

See Chapter 8 *Diagnostic Tools*, section *Syslog Mode* for a detailed explanation of the **Syslog** mode options.

Error Handling Mode

The **Error Handling** mode determines how the handset will behave when an error occurs. The **Halt on Error** option will cause the handset to stop operating if an error message is received. Unless the error is a fatal one, normal operation may be resumed by power-cycling the handset. The **Restart on Error** option will cause the handset to make every effort to reboot quietly and quickly to standby mode. In either scenario, a call in progress will be lost. **Restart On Error** should be used unless specific error conditions are being investigated.

Error detail may be shown on the display, captured by the syslog server and may also be available for downloading with the Handset Administration Tool. An error memory dump can be taken and sent to Customer Service for escalation and analysis.

Restore Defaults

The Restore Defaults option will set all user and administrative parameters except Telephony Protocol to their factory defaults.

Demos

The **Graphics Demo** option starts a demonstration of the handset's OAI graphical capabilities immediately upon selection.

Admin Menu Default Table

When the **Restore Defaults** option is selected, administrative parameters will be reset to their factory defaults as shown in the table below. The **Telephony Protocol** setting will not change. User parameters will be reset per the user-defined preferences default settings table in the next section.

Menu option	Setting	Sub-option	Sub-sub-option	Default
Phone Config				
	PTT/Emerg. Button	Emergency Dial		Disabled
		PTT		Disabled
		[if enabled]	Allowed Channels	[all]
			Name Channels	[None set]
			Priority Channel	Disabled
	Time Zone			GMT
	Daylight Saving			DST No Adjust
	Password			Enabled
	Change Password			[n/a]
	SIP Registration			[None set]
	Clear Regist.			[n/a]
	OAI			Enabled
	Location Service			
		RTLS		Disabled
		Transmit Interval		10 minutes
		Location Server IP		[None set]
		ELP Port		8552
Network Config	IP Addresses			Use DHCP
	SSID*			[None set]
	WLAN Settings	Custom/Security		None
		Custom/QoS	WEP Key Length	40 bit
			QoS (Mode)	SVP
			QoS (DSCP tabs)	WT in call = 46 WT standby = 26

Menu option	Setting	Sub-option	Sub-sub-option	Default
				Other = 0
		Cisco FSR	Username Password	[none set]
	Reg. Domain*			[none set]
		802.11 mode		b & b/g mixed
		Transmit Power		30 mW (15 dBm)
Diagnostics	Run Site Survey			[n/a]
	Diagnostics			Disabled
	Syslog Mode			Disabled
	[Error Handling Mode]			Restart on Error

*Minimum requirements for functionality after Restore Defaults:
Set SSID to an available AP and set Regulatory Domain to 01.

User-Defined Preferences

The SpectraLink 8020/8030 Wireless Telephone features a configuration menu ("Config menu") that is available to the user to configure user preferences and display handset information. The Config menu is opened by pressing the **Cfg** softkey from standby mode. See the *SpectraLink 8020/8030 Wireless Telephone and Accessories User Guide*.

Config Menu

Config menu	2nd level	3rd level	4th level	5th level	6th level
Lock Keys					
User Profiles	Silent Vibrate Loud Soft Custom				
		Set as Active			
		Ring Settings	Telephone Ring Message Alert 1 Message Alert 2		
				Ring Cadence	Off PBX Continuous Short Pulse Long Pulse
				Ring Tone	Tones 1-10
				Ring Volume	Volume ■■■■■■■
				Vibrate Cadence	Off PBX Continuous Short Pulse Long Pulse

Config menu	2nd level	3rd level	4th level	5th level	6th level
		Noise Mode[1]	Normal High Severe		
		Ring in Headset Ring in Speaker			
		Warning Tones Disable/Enable			
		Key Tones Disable/Enable			
		PTT Disable/Enable			
Phone Settings	Keypad Autolock	Disable 5 Seconds 10 Seconds 20 Seconds			
	Display Contrast	Set Contrast			
	Use Hearing Aid Use No Hearing Aid				
	Play Startup Song Inhibit Song				
	Predial Disable/Enable				

[1] High and Severe noise modes increase microphone, speaker, and ring volume settings above Normal mode baseline. All measures are approximate.

	Microphone	In-ear speaker	Ring volume
High	+12dB	+6dB	+3dB
Severe	+18dB	+12dB	+6dB

Config menu	2nd level	3rd level	4th level	5th level	6th level
Push-to-talk *	Default Channel	Channel 1 …. Channel 24			
	Subscribed Channels	Channel 1 Channel 2 Channel 3 …. Channel 24			
	PTT Audio Volume	Audio Volume ■■■■■■■			
	PTT Tone Volume	Tone Volume ■■■■■■■			
	PTT Vibrate Disable/Enable				
System Info	Phone IP Address				
	Alias IP Address				
	SVP IP Address				
	OAI IP Address				
	Firmware Version				
	Emergency Dial *	Emergency Number Emergency Name			

* **Push-to-talk** and **Emergency Dial** only appear if enabled.

Default settings

The profile options on the standby menu may be reset to their default values by the **Restore Defaults** option in the **Admin** menu. These are the default settings:

Setting/profile	Silent	Vibrate	Soft	Loud	Custom
Ring Cadence	Off	Off	PBX	PBX	PBX
Ring Tone	Tone 1	Tone 1	Tone 1	Tone 1	Tone 1
Ring Volume	1	1	3	7	5
Vibrate Cadence	Off	PBX	Off	Off	PBX
Ring Delay	0	0	0	0	5
Noise Mode	Normal	Normal	Normal	Normal	Normal
Headset/Speaker	Speaker	Speaker	Speaker	Speaker	Speaker
Key Tones	Off	Off	On	On	On
Warning Tones	Off	Off	Off	Off	Off
Push-to-talk	Off	Off	On	On	On
PTT Vibrate	Disabled	Disabled	Disabled	Disabled	Disabled
Emergency Dial	On	On	On	On	On

Push-to-talk must be enabled by the system administrator before it can be activated by the user. If it is not enabled, then it will not appear on the Config menu and will not be "On" for any profile.

PTT Vibrate is available only when Push-to-talk has been enabled by the system administrator.

Emergency Dial must be enabled by the system administrator. If enabled, it will be "On" (or available for use) in every profile.

WPA2 Enterprise PEAP Certificate Enrollment and EAP-FAST Manual PAC Provisioning

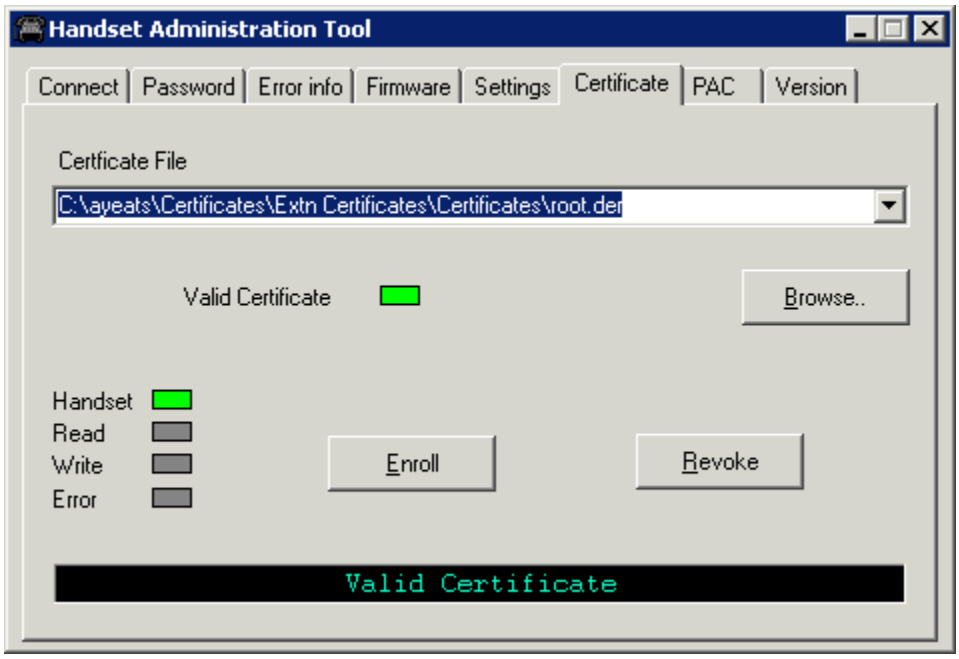
The Handset Administration Tool (HAT) is used for enrolling a handset with a PEAP certificate or manually provisioning PAC files.

PEAP

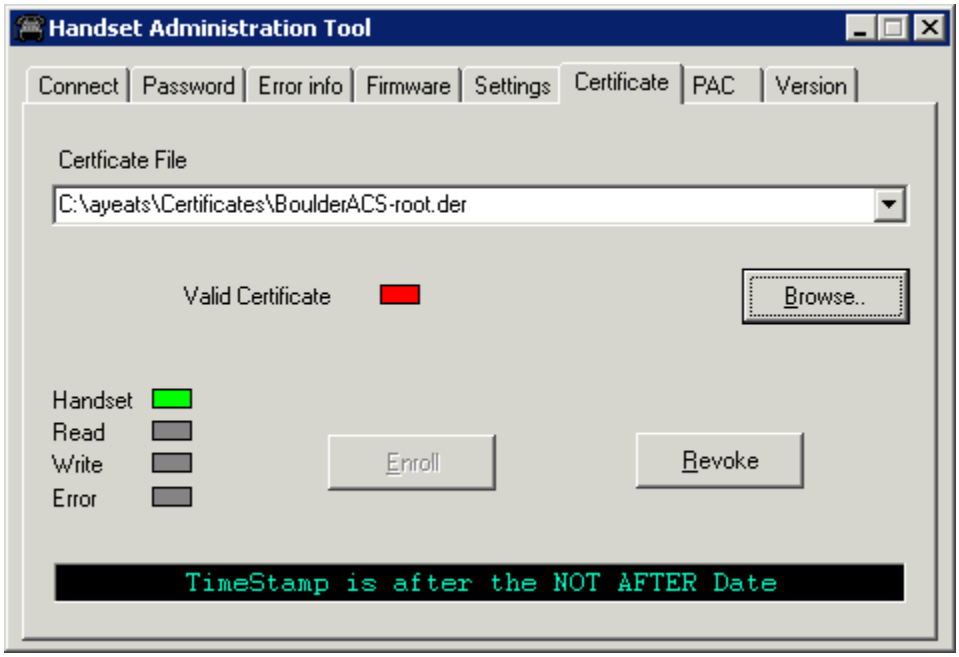
The Handset Administration Tool (HAT) is used for enrolling a handset with a PEAP certificate in DER format. Only the DER certification format is supported. All other certificate formats need to be converted into the DER format prior to enrolling the handset.

Choose the **Certificate** tab and use the file browser to identify the certificate to be loaded. Once chosen, HAT will perform a rudimentary check on the file to make sure the format is DER and that the certificate date is valid. If these tests pass, HAT will indicate that it is valid and enable the **Enroll** button. Click **Enroll** to install the certificate onto the handset.

The screen below shows a valid certificate that has been identified with the file browser.



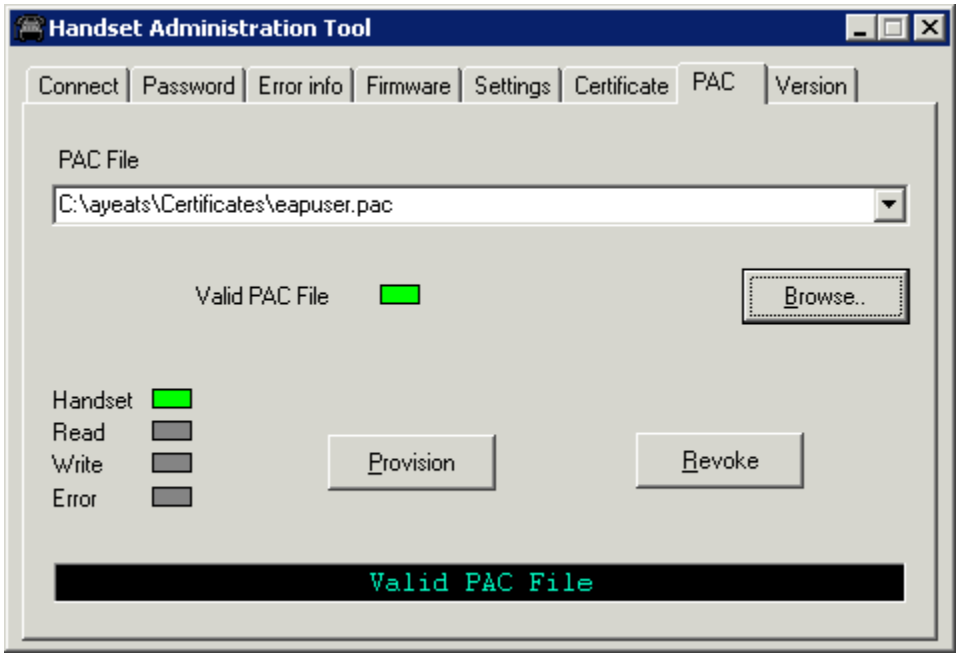
The screen below shows a certificate chosen with the file browser, but found to be invalid because it has expired.



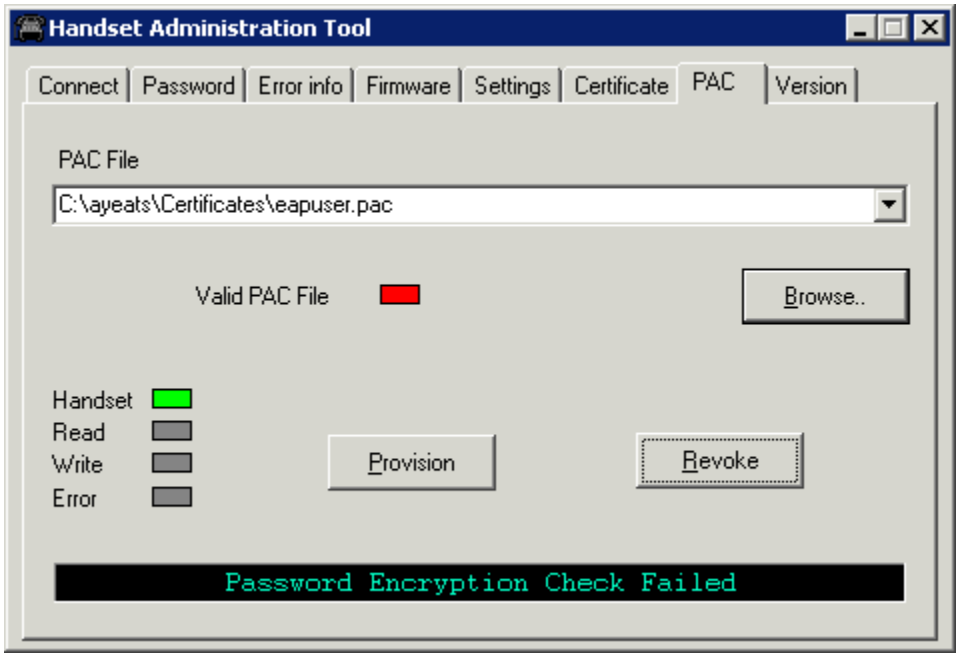
EAP-FAST

For EAP-FAST, HAT is also used for manually provisioning a handset with a Protected Access Credential (PAC). Choose the PAC file with the file browser. The user will be prompted to enter the password used to generate the PAC as part of its validation process. Once the PAC is considered to be valid, the **Provision** button will be available for installing the PAC onto the handset.

The screen below shows a valid PAC identified with the file browser after a valid password has been entered.



The two screens below show the result of entering the wrong password.



If anonymous in-band PAC provisioning is enabled on the RADIUS server, then it is not necessary to download PAC files through HAT. The phone will automatically re-acquire credentials from the RADIUS server over the air.

3

Software License and Protocol Management

SpectraLink 8020/8030 Wireless Telephones support a number of different IP protocol integrations. All SpectraLink 8020/8030 Wireless Telephones are shipped from Polycom with a generic software load that allows them to associate to a wireless LAN and download functional software from a TFTP server. **The handsets will not function properly without downloading appropriate software.**

The following details the process to properly configure SpectraLink 8020/8030 Wireless Telephones and download software via over-the-air file transfer.

Minimum System Requirements

- A wireless LAN must be properly configured and operational through the use of 802.11a/b/g/n wireless APs. Consult the *VIEW Configuration Guide* for the appropriate make/model of WLAN.
- A TFTP must be available on the network in order to load the appropriate software into the handsets. The current handset software must be installed in the proper TFTP download directory.
- If SVP is used for QoS, the SVP Server must be installed and properly configured.
- Software versions required, if SVP and/or OAI are used:

Component	Version
SpectraLink 8000 SVP Server	17x.034 or higher
OAI Server MOG 600	54.032 or higher
OAI Server MOG 700	82.019 or higher

- If Wi-Fi Standard QoS is used, then each AP must be configured for such features as WMM-Power Save; WMM-Admission

Control; proper EDCA parameters; DSCP mapping for voice and control traffic; call admission control and Proxy ARP. Consult the appropriate *VIEW Configuration Guide* for these settings.

- If WPA2-Enterprise is used, then all portions of the Public Key Infrastructure (PKI) need to be installed and configured properly in order acquire the network.
- An approved SIP call server must be installed and operational on the LAN. A complete list of approved product can be found on the Polycom website at http://www.polycom.com/support/voice/wi-fi/feature_lists/spectralink_8020_8030_sip_featurematrix.html

Minimum Configuration Process

1. Download the latest SpectraLink 8020/8030 Wireless Telephone IP software from http://www.polycom.com/usa/en/support/voice/wi-fi/spectralink_8030_wireless.html.
2. Load the latest version of the SIP code and place it on the TFTP server and ensure the TFTP server is started. The slnk_cfg.cfg is downloaded first by the phone, and defines the SIP code files that will be subsequently downloaded. Be sure to use the slnk_cfg.cfg file that comes with the latest version of the SIP code and do not change the order of the files within the slnk_cfg.cfg.

   The following six files are included in the typical SIP software package.

Description	Filename
Configuration file	slnk_cfg.cfg
PHINTL (language translation)	pi1400sp.bin
USB downloader	pd14udsp.bin
Over-The-Air Downloader (OTADL)	pd14odsp.bin
OTADL Shim	pd14shim.bin
Functional (telephony protocol)	pd14csp.bin

3. Use the Handset Administration Tool to set up the configuration of each handset to meet all essential requirements. If not using the Handset Administration Tool, ensure the following parameters are correctly set in the **Admin** menu for each handset: See Chapter 2 *SpectraLink 8020/8030 Wireless Telephone Configuration* for detailed configuration instructions.
   - If statically assigning IP addresses, ensure that the **Phone IP**, **Subnet Mask**, and **Default Gateway** information are accurate. If using a DHCP Server, ensure that the DHCP option is set.
   - Ensure the handset has properly configured **SSID** and **Reg Domain** information.
   - Ensure the **Telephony Protocol** menu option is set to **36**. This ensures the handset will check for the proper SRP files each time it powers on.
   - Ensure security settings are properly programmed.

4. Configure handset security settings to match AP configuration and RADIUS server settings. If WPA2-Enterprise security is used, credentials will need to be installed onto the handset. For EAP-FAST, the PAC file needs to be provisioned and for PEAP the handset will need to be enrolled with a certificate (requires use of the HAT). See the *WPA2 Enterprise PEAP Certificate Enrollment and EAP-FAST Manual PAC Provisioning* section in this guide for details.
5. Configure the QoS handset mode to match the AP and site QoS plan. Follow the *VIEW Configuration Guide* for the appropriate make/model of WLAN.
6. Power cycle the handset.
7. The SIP code will now download to the handset. The status bar will increment fully across the display for each function that is being performed in the download process. Upon completion of the update process, the handset will re-boot with the new firmware.

During the second download evolution, the handset receives code from the TFTP server for system configuration and for its own settings. Once this second evolution is complete, the handset is ready to use.

For future software upgrades, simply update the files that are stored on the TFTP server. Each time the handset is powered on, it will check with the TFTP server to ensure it has the proper software version.

4

SIP Integration Factors

CODECs

The SpectraLink 8020/8030 Wireless Telephones are compatible with the G.711µ-law, G.711a-law and G.729 codecs. There is no setting required on the handset.

DHCP

Dynamic Host Configuration Protocol (DHCP) is a standardized protocol that enables clients to be dynamically assigned with various configuration parameters, such as an IP address, subnet mask, default gateway, and other critical network configuration information. DHCP servers centrally manage such configuration data, and are configured by network administrators with settings that are appropriate for a given network environment. The handset will use the following DHCP options if DHCP use is enabled:

Option	Meaning
1	Subnet mask
3	Default gateway
6	DNS server
7	Syslog server logging
15	Domain name
66	TFTP server
151	SpectraLink 8000 SVP Server
152	SpectraLink 8000 OAI Gateway
siaddr	Boot server or next server

DNS

Domain Name System (DNS), an industry-standard protocol, locates computers on an IP-based network. IP networks rely on number-based addresses to move information on the network. However, it is easier to remember user-friendly names than number-based addresses, so it is necessary to translate user-friendly names into

addresses that the network can recognize. The handset will use DNS to automatically translate names into IP addresses for the TFTP server and SpectraLink 8000 SVP Server.

In DHCP mode, the SIP handset will use DNS to look up an address for the logical name “siptftp” to locate the SIP TFTP file server. If this logical name is undefined, then the address specified by option 66 or the boot server/next server (siaddr) field is used for the SIP TFTP server.

Sample DHCP Server Configuration File

A sample DHCP server configuration file is illustrated below. Please note that this is only a sample and will not work on your system as written here. In addition, this file is specific to the ISC DHCP server. Your configuration files must be locally programmed according to your site requirements.

dhcpd.cfg

```
# /etc/dhcpd.conf
#
# Sample configuration file for ISC dhcpd
#
# Type "man dhcp-options" at prompt to get help for these options.
#

# Global parameters start at beginning of file.

# If this DHCP server is the official DHCP server for the local
# network, the authoritative directive should be uncommented.
# This means the DHCP server will send DHCPNAK messages to misconfigured
# clients.
authoritative;

# Use local address if you want the DHCP server to listen for DHCP requests
# on a specified address, rather than requests send to all addresses.
local-address 192.168.0.1;

# define the default gateway / router option 3
option routers 192.168.0.1;

# define the DNS server(s) option 6
option domain-name-servers 192.168.0.1;

# define the SYSLOG server option 7
option log-servers 192.168.0.1;

# define the domain name option 15
option domain-name "polycom.com";

# define the SVP server option code 151 as an IP address.
option svp-server code 151 = ip-address;
```

```
# define the OAI server option code 152 as an IP address.
option oai-server code 152 = ip-address;

# This should  be  the  length  in seconds that will be
# assigned to a lease if the client requesting the lease does not ask
# for a specific expiration time.  86400 seconds is 1 day.
default-lease-time 86400;

# This should be the maximum length in seconds that will  be  assigned
# to a lease.
max-lease-time 86400;

# minimum lease time of 10 minutes
min-lease-time 600;

# You can declare a class of clients and then do address allocation
# based on that.   The example below shows a case where all clients
# in a certain class get addresses in the range 192.168.0.100 to 192.168.0.149,
# and all other clients get addresses in the range 192.168.0.150 to
# 192.168.0.199.

class "SpectraLinkPhones" {
  match if substring (option vendor-class-identifier, 0, 11) = "SpectraLink";
}

# subnet definition also sets netmask option 1
subnet 192.168.0.0 netmask 255.255.255.0 {

  # DHCP lease pool for Polycom SpectraLink phones
  pool {
    allow members of "SpectraLinkPhones";
    range 192.168.0.100 192.168.0.149;

    # define the siaddr / next server field as the alternative TFTP server address
    next-server 192.168.0.1;

    # define the NTP server option 42
    option ntp-servers 192.168.0.1;

    # define the primary TFTP server address option 66
    option tftp-server-name "192.168.0.1";

    # define the SVP server address option 151 if using SVP QoS
    option svp-server 192.168.0.5; # option 151

    # define the OAI server address option 152
    option oai-server 192.168.0.6; # option 152
  }

  # DHCP lease pool for other devices
  pool {
    deny members of "SpectraLinkPhones";
    range 192.168.0.150 192.168.0.199;
    next-server 192.168.0.1;
    option tftp-server-name "192.168.0.1";
```

5

Programming the SIP Handset Features

In order for the handset to function in the SIP environment, it downloads two files from the root directory of the SIP TFTP server during startup. The first file contains generic system information and is downloaded by every handset during the power-up sequence. A second file, unique for each handset, is then downloaded. It contains specific information for each handset such as username, password, and line appearances. Both of these files must be written locally.

Sample files populated with default parameters are provided with the software downloaded from the website. We recommend using these sample files as a starting point and adjusting them according to your system requirements. See the *Sample Configuration Files* section below for the default values.

SIP TFTP Server Configuration Files

The two file types, generic and specific, are identical in format. Any or all of the configuration information can be contained in either file. Any information in the specific file that conflicts with the information in the generic file will take precedence over that in the generic file. Authentication information will be accepted from both files. For ease of administration, it is recommended both file types be utilized.

Guidelines

- The files are in plain text, US-ASCII. The general form of the configuration file data is "parameter = value."
- The generic filename must be SIP_allusers.cfg.
- Each specific filename must have the form of SIP_username.cfg where [username] is as assigned to each individual user by the system administrator. See Chapter 2 *SpectraLink 8020/8030 Wireless*

Telephone Configuration, section *The Admin Menu*, subsection *SIP Registration*.

- Username parameters are: alphanumeric, no spaces, no punctuation, case is ignored, 1-16 characters.
- Generic file information should contain proxy server information and other SIP system data.
- Specific file information should contain data specific to each user such as authentication credentials and line appearance data.
- Some parameter lines accept more than one value, separated by a colon or semicolon character as defined in the following table.
- Any line that begins with a pound sign (#) is ignored.
- In general space characters are ignored. Space characters may be included in string values by replacing the space with "%20" or by enclosing the string in quotes (").
- If necessary, other special characters may be included by using a hexadecimal representation: (%hh) where hh is the representation of the character.
- Lines may appear in any order although maintenance may be simplified by preserving the order in the supplied example file.

Program each of the files according to the following instructions.

The generic file (sip_allusers.cfg)

The generic configuration file provides system information common to all handsets.

The handset-specific files (e.g. sip_3001.cfg)

The handset-specific configuration file provides specific information for the handset to identify itself and communicate to other phones. Each handset must have its own file with a unique filename. You may use the same parameters as the generic file when programming the handset files if you wish to override a common setting.

You must configure a unique handset file for each handset being deployed. Typically each of these files is named with the extension number or name of the person assigned the handset. For example John Doe's handset could have a handset filename of sip_3001.cfg or sip_JohnDoe.cfg.

Proxy server commands

Use the following parameters when programming the configuration files. See the sample configuration files following this table for more detailed information.

Parameter	Value	Description	Notes
PROXYn_ADDR	xxx.xxx.xxx.xxx:pppp or proxyname:pppp	Proxy address. One proxy address is required but additional proxy addresses may be used to register secondary line appearances.	n = 1, 2, 3 xxx.xxx.xxx.xxx = IP4 address pppp = port (optional, 5060 is the default) proxyname = computer name (DHCP only)
PROXYn _DOMAIN	Domain name	Domain served by this proxy server.	n = 1, 2, 3 DOMAIN = [example: spectralink.com] Can be omitted if a specific proxy domain name is not defined at the proxy server. If omitted, defaults to the IP address of the proxy server (see above).
PROXYn_TYPE	Asterisk[2] NEC (NECSIP) Mitel Cisco Call Manager Express or Unified Communications Manager Express. (CCME) PingTel Interactive Intelligence (ININ) Toshiba Cisco Call Manager or Unified Communcations Manager (CCM) 3Com	Specify the manufacturer of each defined proxy server. See sample files for vendor notation.	Used by the handset to perform proxy-specific actions based on known behavior for specific proxy types. Only the three shown values may be used. Omit this parameter if the value is not one of these recognized settings.

2 For up-to-date Asterisk voicemail commands, go to: http://www.voip-info.org/wiki/index.php?page=Asterisk+cmd+VoiceMailMain

Parameter	Value	Description	Notes
PROXYn_ KEEPALIVE_SECS Not used in 8020/8030	0 or 10 to 3600 seconds *default = 0	Specifies that the handset should send keepalives to the PROXYn server.	n = 1, 2, 3 The keepalive interval defaults to ZERO which disables the feature. When specified, the interval can be set to zero or to 10 to 3600 seconds. If a keepalive fails to get a response within the SIP 32 second timeout, then keepalives are terminated until the next successful registration to the proxy. See example file.
PROXYn_ KEYPRESS_2833	*enable disable *default (in example file)	Controls generation of in-stream RFC2833 formatted key press events. Match what is required by your PBX. See RFC2833. See config file example for more information.	n = 1, 2, 3 Must be disabled for OAI.
PROXYn_ KEYPRESS_INFO	enable disable	Controls generation of SIP INFO requests to the SIP server for keypress events. Normally enabled.	n = 1, 2, 3 Must be enabled for OAI.
PROXYn_HOLD_IP0	enable disable	Controls setting of the media stream IP destination address to 0 (zero) when a call is put on hold. See config file example for more information.	n = 1, 2, 3 Use for compatibility with older SIP servers that may not recognize newer stream attribute parameters for HOLD status.
PROXYn_PRACK	enable disable	Enables reliable provisional responses to INVITE requests	n = 1, 2, 3
PROXYn _ MAIL_SUBSCR	name@xxx.xxx.xxx.xxx or sip:name@domain	Contact to whom the handset should subscribe for mail notification. See config file example for more information.	n = 1, 2, 3 name = mail server contact name. xxx.xxx.xxx.xxx = IP4 address. Domain where the mail resides[3].

[3] For mail notifications, in general you will need to define only one contact parameter for each proxy. If the proxy

Parameter	Value	Description	Notes
PROXYn_ MAIL_ACCESS	name@xxx.xxx.xxx.xxx or sip:name@domain	Contact to whom the handset should invite to access the mail center. This is the main voicemail dial number.	n = 1, 2, 3 name = mail server contact name. xxx.xxx.xxx.xxx = IP address Domain where the mail resides.
PROXYn _ MAIL_NOTIFY	name@xxx.xxx.xxx.xxx or sip:name@domain	Contact from whom mail notification originates. See config file example for more information.	n = 1, 2, 3 [4] name = mail server contact name. [5] xxx.xxx.xxx.xxx = IP address. Domain where the mail resides.
PROXYn_ REREG_SECS Not used in 8020/8030	35 seconds to 3600 seconds *default 3600 seconds	The requested expiration interval in REGISTER request messages.	n = 1, 2, 3 If the server has a lower maximum setting or a higher minimum setting than that requested, the server response takes precedence. See example file
PROXYn_FAILOVER IP_ADDRESS	xxx.xxx.xxx.xxx:pppp or proxyname:pppp	The IP address of the Interactive Intelligence failover call server.	n = 1, 2, 3 xxx.xxx.xxx.xxx = IP4 address pppp = port (optional, 5060 is the default) proxyname = computer name (DHCP only)

server automatically creates and renews subscriptions when the handset registers, then only the PROXYn _MAIL_NOTIFY contact need be specified. If the handset must subscribe to a particular contact to get mail notification, then only the PROXYn_MAIL_SUBSCR contact needs to be specified.

[4] Values as above.

[5] For Inter-Tel SIP servers, both PROXYn_MAIL_SUBSCR and PROXYn_MAIL_NOTIFY parameters must be set in the configuration file.

Parameter	Value	Description	Notes
AUTH [see warning note below]	username;password	Credentials. In general credentials are needed for each registered line.[6].	username = The dial number or string that identifies the line appearance. Generally an extension or phone number. password = a secure password created by the system administer which enables a handset to register and/or function.
CODECS	codec1, codec2 e.g. g711u, g711a, g729	Comma-separated list of supported codecs in order of preference.	Defaults to "g711u, g711a". if either is omitted it will be added to the end of the list.
LINEn	username	The dial # or name. All LINEn user names should be unique for a given LINEn_ PROXY. This may be enforced in future software revisions.	n = 1, 2, 3, 4, 5 The registered contact becomes: sip:username@domain
LINEn _PROXY	i	SIP proxy server for this line.	n = 1, 2, 3, 4, 5 i = the number of the proxy server 1, 2, 3. LINEn_PROXY can be omitted if the line is not to be registered and you wish to do direct phone to phone calls.
LINEn _CALLID	callerid	String that displays at the far end.	n = 1, 2, 3, 4, 5 callerid = the text that will display as the caller ID on the called handset.

[6] WARNING: providing credentials by using the AUTH parameters in the configuration files is a security risk and should be avoided by entering usernames and passwords in **Admin** menu or by allowing the user to login at startup time. Credentials entered here are in plain text and accessible by anyone who can access the TFTP server files. Credentials stored in the SIP server or in the handsets are protected.

Parameter	Value	Description	Notes
FAVORITE	Dialstring;identifier;LINEn	Phonebook list of numbers accessible from the Favorites menu. Favorites in the allusers file will be present in the Favorites on all handsets. See config file example for more information.	Up to 15 entries permitted which may be divided between generic and phone specific files. Dialstring = complete SIP URI or local extension # Identifier = name. if omitted, the dial string appears on Favorites menu. LINEn = can be omitted if dialing can be done on any registered line. Usually omitted but if present, the number will be dialed on the programmed line.

Sample SIP Configuration Files

Sample SIP configuration files are illustrated below. These files are available as a download from the software updates site and may be customized for your application. Please note that these are merely samples and will not work on your system as written here or as downloaded. Your configuration files must be locally programmed according to your site requirements.

SIP_allusers.cfg

```
# SIP ALL USERS Configuration file example

# Configuration file format example
# Maximum number of characters allowed per line (excluding comments) in this configuration file
is 121.
#-------------------------------------------------------------------------------------------#
#-------------------------------------------------------------------------------------------#

# Codec preference order only.  This does not enable/disable codecs. (Optional)
# can be G.711-ulaw, g.711u, G.711U, g711u, G.711U, g729, G729, G.729, g729ab, g729AB
# if g711u is omitted it will be added to end of list.
# if g711a is omitted it will be added to end of list after u.
CODECS = g711u, g711a

#-------------------------------------------------------------------------------------------#
#
# PROXY settings... At least one is required and up to three may be specified.
#                   Where one is specicifed, all proxy settings must share the
#                   same numbered prefix (i.e. PROXY1_...)
#

# One PROXYn_TYPE (PBX/Call Server) entry is required, additional ones are optional as you
# can register secondary line appearances with other PROXY servers
# Uncomment Your Proxy Type from the list below
#
#PROXY1_TYPE           = Asterisk
#PROXY1_TYPE           = NECSIP
#PROXY1_TYPE           = MITEL
#PROXY1_TYPE           = CCME
#PROXY1_TYPE           = PINGTEL
#PROXY1_TYPE           = ININ
#PROXY1_TYPE           = TOSHIBA
#PROXY1_TYPE           = CCM
#PROXY1_TYPE           = 3COM
#PROXY1_TYPE           = SHORETEL
#PROXY1_TYPE           = DELTAPATH

#-------------------------------------------------------------------------------------------#
#-------------------------------------------------------------------------------------------#


## FOR EACH PROXY TYPE LISTED ABOVE POLYCOM HAS FOUND THE FOLLOWING
## VALUES TO WORK WELL DURING TESTING, THOUGH YOUR SPECIFIC
## CONFIGURATION MAY VARY. UNCOMMENT OUT THE FIELDS PRECEEDED BY A
## SINGLE # TO ACCEPT THESE VALUES
```

```
## ADDITIONAL INFORMATION ABOUT EACH OF THESE FIELDS AS WELL AS SPECIFIC
## CONFIGURATION EXAMPLES CAN BE FOUND FURTHER DOWN IN THIS FILE

#-------------------------------------------------------------------------------------------#
#-------------------------------------------------------------------------------------------#

## FOR PROXY1_TYPE = NECSIP

#PROXY1_ADDR     = 172.29.102.122:5060       # replace the ip address with your Sip Server's
Address
#PROXY1_KEYPRESS_2833 = enable
#PROXY1_KEYPRESS_INFO = disable
#PROXY1_HOLD_IP0 = disable
#PROXY1_PRACK = enable
#PROXY1_REREG_SECS=3600
#PROXY1_KEEPALIVE_SECS=14
#PROXY1_DOMAIN = necpolysip:5060             # Replace this with your SIP Domain's name
#PROXY1_CALLID_PER_LINE = disable
#PROXY1_MAIL_ACCESS = 7999                   # Put Your Voice Mail Sytem's Pilot Number here
#PROXY1_CONF_IP_ADDRESS       = 172.29.102.131
## For each proxy of type NECSIP, one PROXYn_CONF_IP_ADDRESS is required
## This value is the address of NEC PBX's IP PAD card.

#-------------------------------------------------------------------------------------------#

## FOR PROXY1_TYPE = ASTERISK

#PROXY1_ADDR     = 172.29.65.6:5060          # replace the ip address with the Asterisk Server's
Address
#PROXY1_KEYPRESS_2833 = enable
#PROXY1_KEYPRESS_INFO = disable
#PROXY1_HOLD_IP0 = disable
#PROXY1_PRACK = enable
#PROXY1_REREG_SECS=3600
#PROXY1_KEEPALIVE_SECS=14
#PROXY1_DOMAIN = axlx.engr.local             # Replace this with your SIP Domain's name
#PROXY1_CALLID_PER_LINE = disable
#PROXY1_MAIL_ACCESS = 7999                   # Put Your Voice Mail Sytem's Pilot Number here

#-------------------------------------------------------------------------------------------#

## FOR PROXY1_TYPE = MITEL

#PROXY1_ADDR     = 172.29.102.160:5060       # replace the ip address with your PBX's Address
#PROXY1_KEYPRESS_2833 = enable
#PROXY1_KEYPRESS_INFO = disable
#PROXY1_HOLD_IP0 = enable
#PROXY1_PRACK = enable
#PROXY1_REREG_SECS=3600
#PROXY1_KEEPALIVE_SECS=14
#PROXY1_DOMAIN =                             # Put Your SIP Domain's Name Here
#PROXY1_CALLID_PER_LINE = disable
#PROXY1_MAIL_ACCESS = 7000                   # Put Your Voice Mail Sytem's Pilot Number here

#-------------------------------------------------------------------------------------------#

## FOR PROXY1_TYPE = CCME

#PROXY1_ADDR     = 172.24.144.107:5060       # replace the ip address with the UCME's Address
#PROXY1_KEYPRESS_2833 = disable
#PROXY1_KEYPRESS_INFO = enable
#PROXY1_HOLD_IP0 = enable
#PROXY1_PRACK = enable
#PROXY1_REREG_SECS=3600
#PROXY1_KEEPALIVE_SECS=14
```

```
#PROXY1_DOMAIN =                              # Put Your SIP Domain's Name Here
#PROXY1_CALLID_PER_LINE = enable
#PROXY1_MAIL_ACCESS = 7999                    # Put Your Voice Mail Sytem's Pilot Number here

#-------------------------------------------------------------------------------------#

## FOR PROXY1_TYPE = PINGTEL

#PROXY1_ADDR     = 172.24.144.127:5060        # replace the ip address with the Pingtel's Address
#PROXY1_KEYPRESS_2833 = enable
#PROXY1_KEYPRESS_INFO = disable
#PROXY1_HOLD_IP0 = enable
#PROXY1_PRACK = enable
#PROXY1_REREG_SECS=3600
#PROXY1_KEEPALIVE_SECS=14
#PROXY1_DOMAIN = asia.polycom.com             # Put Your SIP Domain's Name Here
#PROXY1_CALLID_PER_LINE = disable
#PROXY1_MAIL_ACCESS = 101                     # Put Your Voice Mail Sytem's Pilot Number here

#-------------------------------------------------------------------------------------#

## FOR PROXY1_TYPE = ININ

#PROXY1_ADDR     = 172.24.144.135:8060        # replace the ip address with the II's Address and
port number
#PROXY1_FAILOVERIP = 172.24.144.136:8060      # replace the ip address with the secondary ININ IP
address.
#PROXY1_KEYPRESS_2833 = enable
#PROXY1_KEYPRESS_INFO = disable
#PROXY1_HOLD_IP0 = enable
#PROXY1_PRACK = enable
#PROXY1_REREG_SECS=3600
#PROXY1_KEEPALIVE_SECS=14
#PROXY1_DOMAIN =                              # Put Your SIP Domain's Name Here
#PROXY1_CALLID_PER_LINE = disable
#PROXY1_MAIL_ACCESS = 7999                    # Put Your Voice Mail Sytem's Pilot Number here

#-------------------------------------------------------------------------------------#

## FOR PROXY1_TYPE = TOSHIBA

#PROXY1_ADDR     = 172.29.102.106:5060        # replace the ip address with the CIX100's Address
#PROXY1_KEYPRESS_2833 = enable
#PROXY1_KEYPRESS_INFO = disable
#PROXY1_HOLD_IP0 = disable
#PROXY1_PRACK = enable
#PROXY1_REREG_SECS=3600
#PROXY1_KEEPALIVE_SECS=14
#PROXY1_DOMAIN =                              # Put Your SIP Domain's Name Here
#PROXY1_CALLID_PER_LINE = disable
#PROXY1_MAIL_ACCESS = 290                     # Put Your Voice Mail Sytem's Pilot Number here

#-------------------------------------------------------------------------------------#

## FOR PROXY1_TYPE = CCM

#PROXY1_ADDR     = 172.24.144.103:5060        # replace the ip address with the CCM's Address
#PROXY1_KEYPRESS_2833 = enable
#PROXY1_KEYPRESS_INFO = disable
#PROXY1_HOLD_IP0 = disable
#PROXY1_PRACK = enable
#PROXY1_REREG_SECS=3600
#PROXY1_KEEPALIVE_SECS=14
#PROXY1_DOMAIN =                              # Put Your SIP Domain's Name Here
#PROXY1_CALLID_PER_LINE = enable
```

```
#PROXY1_MAIL_ACCESS = 9999                  # Put Your Voice Mail Sytem's Pilot Number here

#-------------------------------------------------------------------------------------#

## FOR PROXY1_TYPE = 3COM

#PROXY1_ADDR     = 172.29.102.190:5060      # replace the ip address with the 3COM's Address
#PROXY1_KEYPRESS_2833 = enable
#PROXY1_KEYPRESS_INFO = disable
#PROXY1_HOLD_IP0 = enable
#PROXY1_PRACK = enable
#PROXY1_REREG_SECS=3600
#PROXY1_KEEPALIVE_SECS=14
#PROXY1_DOMAIN =                            # Put Your SIP Domain's Name Here
#PROXY1_CALLID_PER_LINE = disable
#PROXY1_MAIL_ACCESS = 5000                  # Put Your Voice Mail Sytem's Pilot Number here

#-------------------------------------------------------------------------------------#

## FOR PROXY1_TYPE = DELTAPATH

#PROXY1_ADDR     = 10.240.240.226:5060      # replace the ip address with the Asterisk Server's
Address
#PROXY1_KEYPRESS_2833 = enable
#PROXY1_KEYPRESS_INFO = disable
#PROXY1_HOLD_IP0 = disable
#PROXY1_PRACK = enable
#PROXY1_REREG_SECS=3600
#PROXY1_KEEPALIVE_SECS=14
#PROXY1_DOMAIN = axlx.engr.local            # Replace this with your SIP Domain's name
#PROXY1_CALLID_PER_LINE = disable
#PROXY1_MAIL_ACCESS = 7999                  # Put Your Voice Mail Sytem's Pilot Number here

#-------------------------------------------------------------------------------------#

## FOR PROXY1_TYPE = SHORETEL

#PROXY1_ADDR     = 172.29.102.212:5060      # replace the ip address with the Shoretel's Address
#PROXY1_KEYPRESS_2833 = enable
#PROXY1_KEYPRESS_INFO = disable
#PROXY1_HOLD_IP0 = disable
#PROXY1_PRACK = enable
#PROXY1_REREG_SECS=3600
#PROXY1_KEEPALIVE_SECS=14
#PROXY1_DOMAIN = asia.polycom.com           # Put Your SIP Domain's Name Here
#PROXY1_CALLID_PER_LINE = disable
#PROXY1_MAIL_ACCESS = 102                   # Put Your Voice Mail Sytem's Pilot Number here

#########################################################################################
##### This section describes how to add Favorites ######################################

#   Favorites in the allusers file will be present in the favorites on all phones
#   The username can be blank and can include escaped chars
#   Useful features can be included such as call forwarding or dialing voicemail
#FAVORITE = "1234"; "Site Security"
#FAVORITE = "*98"; "Call Forwarding"
#
#   Favorites can also be configured to prompt users to enter more digits. Users will
#   be prompted with characters inside the <>'s.
#   In the below example if the Feature Access Code for call forwarding is #21
#   When the user selects the Favorites option and then Call Forward they would
#   see "Call Forward Enter Destination:"
#   They would then have a chance to enter the fwd destination before pressing the send key
#FAVORITE =  #21<Enter Destination:>; "Call Forward"
#   In the example below the user would be prompted "Call Pickup Pickup Number:
```

```
#   to enter a call pickup number # for a call pickup Feature Access Code starting with *5
#FAVORITE =  *5<Pickup Number:>; "Call Pickup"
# If user wants to add a comment for a FAVORITE, it should be added on the next line (not on the
same line where a FAVORITE is defined).

##############################################################################################
##### THIS SECTION EXPLAINS THE PROXY_N PARAMETERS IN MORE DETAIL AND GIVES FORMAT EXAMPLES ####

# One PROXYn_ADDR (PBX/Call Server) entry is required, additional ones are optional as you
#  can register secondary line appearances with other PROXY servers
#
#PROXY1_ADDR     = 172.29.102.131:5060
#PROXY2_ADDR     = 172.29.0.140:5060

#--------------------------------------------------------------------------------------------#


# For each proxy of type NECSIP, one PROXYn_CONF_IP_ADDRESS is required. This value is
# the address of NEC PBX's IP PAD card.
#
#PROXY1_CONF_IP_ADDRESS       = 172.29.102.131

#--------------------------------------------------------------------------------------------#


# To test ININ Redundancy PROXY1_FAILOVERIP is required. This value is the secondary IP address
# of the ININ server. If the primary server fails we need to use this address to make the calls.
#
#PROXY1_FAILOVERIP = 172.24.144.136

#--------------------------------------------------------------------------------------------#
#ProxyDomain can be omitted if a specific proxy domain name is not defined at the
# proxy server. If omitted, the ProxyDomain defaults to the IP address of the
# proxy server.
# (below are examples of different ways to specify a domain)
#PROXY1_DOMAIN = plcmengr.com
#PROXY1_DOMAIN = 10.0.0.138
#PROXY1_DOMAIN = axlx.engr.local

#--------------------------------------------------------------------------------------------#

# PROXYn_MAIL_SUBSCR is who we should subscribe to for mail center notifications
# This is needed only if the user is not subscribed automatically at registration.
# It is almost never required in current versions of Asterisk to specify this.
# If you are using Asterisk (non-business edition) before v1.2, this is necessary.
# This example is actually specific for a line number:3001
#PROXY1_MAIL_SUBSCR = sip:3001@vmail.asterisk.com

#--------------------------------------------------------------------------------------------#

# PROXYn_MAIL_ACCESS is the main voicemail dial number
# Examples:
#PROXY1_MAIL_ACCESS = 7999
# PROXY1_MAIL_ACCESS = sip:7999@10.0.0.138
# PROXY1_MAIL_ACCESS = 7999@10.0.0.138
# PROXY1_MAIL_ACCESS = 7999

#--------------------------------------------------------------------------------------------#

#PROXYn_KEYPRESS_2833 controls generation of in-stream RFC2833 formatted key
# press events. Normally you want this to be disabled for Asterisk but it depends
# on your configuration and what you want to be able to do.
# If you are going to do OAI integration, this must be disabled.
# The default is disable
#PROXY1_KEYPRESS_2833 = disable
```

```
#-------------------------------------------------------------------------------------#

#PROXYn_KEYPRESS_INFO controls generation of SIP INFO requests to the SIP server
# for keypress events.  Normally you want this to be enabled.
# If you are going to do OAI integration, this must be enabled.
# The default is enable
#PROXY1_KEYPRESS_INFO = enable

#-------------------------------------------------------------------------------------#

# PROXYn_HOLD_IP0 controls setting of media stream IP destination to 0.0.0.0 when
# a call is put on hold.
# PROXYn_HOLD_IP0 is not required for current versions of Asterisk.
#  For older PBXs that require this, set this to enable
#PROXYn_HOLD_IP0 = enable

#-------------------------------------------------------------------------------------#

# PROXYn_PRACK enables ACK'd provisional responses to INVITE requests.  The PRACK
#  mechanism will be used if this switch is enabled and the Proxy server specifies
#  support for the PRACK mechanism.  PRACK is NOT SUPPORTED in current versions of
#  Asterisk, but is to be supported on subsequent versions.  PRACK should not be
#  required on local area networks.
#PROXY1_PRACK = disable

#-------------------------------------------------------------------------------------#



# PROXYn_KEEPALIVE_SECS specifies that the phone should send Keep Alives to the
#  PROXYn server.  It can be set to 0 or anywhere from 10 to 3600 seconds.
#  The default value (which is applied if no parameter is supplied in this file) is
#  0 which means the phone will not send keep_alives to PROXYn.
#
#  If the phone failes to get a keepalive response within the SIP 32 second
#  timeout, the keepalives are terminated for that PROXY until the next successful
#  registration to the PROXY.
#
#  This parameter is REQUIRED on Asterisk Business Edition with the Polycom 8002
#  phone. For Polycom 8020/8030 phones, this parameter is required when they are
#  operating in WI-FI standard QoS mode.This is because Linux, the OS running Asterisk,
#  has a ARP Cache flushing mechanism. This feature serves to refresh the ARP Cache for the 8002
phones.
#  For 8020 and 8030 phones, operating in SVP mode ARP Cache is refreshed by the SVP server.
#  If the phones are operating in standard based QoS method ARP cache refresh has to be done by
phone.
#
#  The value of this parameter for phones should be just less than the
#  minimum ARP Cache flushing time on the Linux box running Asterisk.  For Redhat
#  this minimum flushing time is 15 seconds, so the parameter needs to be set for
#  14 seconds or less.  For other Linux Distributions, you may have to determine
#  what this minimum value is, however 14 seconds should work fine.
#
#  The lower this setting, the more the impact on the phone's standby battery life.
#  (8002 phones running version 130.003 and earlier code ignore this parameter if
#  present)
#  8020/8030 phones running version 131.017 and earlier code ignore this parameter if
#  present)
#PROXY1_KEEPALIVE_SECS=14

#-------------------------------------------------------------------------------------------#

# PROXYn_REREG_SECS specifies the the re-registration interval for a PROXY.  This
#  is the requested expiration interval sent in the REGISTER request message.  It can
```

```
#  be set to anything between 35 and 3600 seconds.
#  The default value (which is applied if no parameter is supplied in this file) is
#  3600 which means the phone will attempt to register every 3580 seconds, if the
#  server's response interval doesn't take precedence (see below).
#
#  If the server has a lower maximum setting or a higher minimum setting that
#  this value then the server's response will take precedence and this parameter
#  will be ignored.
#
#  The phone will always attempt to re-register with the PROXY 20 seconds prior to
#  the expiration interval.  Thus, if this parameter is set to 35 seconds, and the
#  server's response interval doesn't take precedence, then the phone will attempt
#  to re-register every 15 seconds.
#
#  The lower this setting, the more the impact on the 8002's standby battery life.
#(8002 phones running version 130.003 and earlier code ignore this parameter if
# present)
#PROXY1_REREG_SECS=3600

#-------------------------------------------------------------------------------------------#


# PROXYn_CALLID_PER_LINE controls sending of same Call-ID header
# field for registrations sent to a particular registrar."
# If this is enable we will send  Call-ID headers differently.
# This may be needed for Mitel 3300 Controller software prior to Release 9
#PROXYn_CALLID_PER_LINE = enable
```

Sample handset-specific file

```
# SIP Extension Specific Configuration file format example

# Maximum number of characters allowed per line (excluding comments) in this configuration file
is 121.

#  ////////////////////////////////////////////////////////////////////////////////////////////#
#  //////  Items IN THE PROXY SECTION should be in the sip_allusers.cfg file with
#  //////   items uncommented in this file only for overriding a setting for a
#  //////   particular user.
#  ////////////////////////////////////////////////////////////////////////////////////////////#



# Codec preference order only.  This does not enable/disable codecs. (Optional)
# can be G.711-ulaw, g.711u, G.711U, g711u, G.711U, g729, G729, G.729, g729ab, g729AB
# if g711u is omitted it will be added to end of list.
# if g711a is omitted it will be added to end of list after u.
#CODECS = g711u, g711a

#-------------------------------------------------------------------------------------------#

#
# PROXY settings... At least one is required and up to three may be specified.
#                   Where one is specicifed, all proxy settings must share the
#                   same numbered prefix (i.e. PROXY1_...)
#

# One PROXYn_TYPE (PBX/Call Server) entry is required, additional ones are optional as you
# can register secondary line appearances with other PROXY servers
# Uncomment Your Proxy Type from the list below
#
#PROXY1_TYPE           = Asterisk
#PROXY1_TYPE           = NECSIP
#PROXY1_TYPE           = MITEL
#PROXY1_TYPE           = CCME
#PROXY1_TYPE           = PINGTEL
#PROXY1_TYPE           = ININ
#PROXY1_TYPE           = TOSHIBA
#PROXY1_TYPE           = CCM
#PROXY1_TYPE           = 3COM
#PROXY1_TYPE           = SHORETEL
#PROXY1_TYPE           = DELTAPATH

#-------------------------------------------------------------------------------------------#
#-------------------------------------------------------------------------------------------#


## FOR EACH PROXY TYPE LISTED ABOVE POLYCOM HAS FOUND THE FOLLOWING
## VALUES TO WORK WELL DURING TESTING, THOUGH YOUR SPECIFIC
## CONFIGURATION MAY VARY. UNCOMMENT OUT THE FIELDS PRECEEDED BY A
## SINGLE # TO ACCEPT THESE VALUES
## ADDITIONAL INFORMATION ABOUT EACH OF THESE FIELDS AS WELL AS SPECIFIC
## CONFIGURATION EXAMPLES CAN BE FOUND FURTHER DOWN IN THIS FILE

#-------------------------------------------------------------------------------------------#
#-------------------------------------------------------------------------------------------#


## FOR PROXY1_TYPE = NECSIP

#PROXY1_ADDR     = 172.29.102.122:5060       # replace the ip address with your Sip Server's
Address
```

```
#PROXY1_KEYPRESS_2833 = enable
#PROXY1_KEYPRESS_INFO = disable
#PROXY1_HOLD_IP0 = disable
#PROXY1_PRACK = enable
#PROXY1_REREG_SECS=3600
#PROXY1_KEEPALIVE_SECS=14
#PROXY1_DOMAIN = necpolysip:5060            # Replace this with your SIP Domain's name
#PROXY1_CALLID_PER_LINE = disable
#PROXY1_MAIL_ACCESS = 7999                  # Put Your Voice Mail Sytem's Pilot Number here
#PROXY1_CONF_IP_ADDRESS       = 172.29.102.121
## For each proxy of type NECSIP, one PROXYn_CONF_IP_ADDRESS is required
## This value is the address of NEC PBX's IP PAD card.

#-------------------------------------------------------------------------------------------#

## FOR PROXY1_TYPE = ASTERISK

#PROXY1_ADDR     = 172.29.65.6:5060         # replace the ip address with the Asterisk Server's
Address
#PROXY1_KEYPRESS_2833 = enable
#PROXY1_KEYPRESS_INFO = disable
#PROXY1_HOLD_IP0 = disable
#PROXY1_PRACK = enable
#PROXY1_REREG_SECS=3600
#PROXY1_KEEPALIVE_SECS=14
#PROXY1_DOMAIN = axlx.engr.local            # Replace this with your SIP Domain's name
#PROXY1_CALLID_PER_LINE = disable
#PROXY1_MAIL_ACCESS = 7999                  # Put Your Voice Mail Sytem's Pilot Number here

#-------------------------------------------------------------------------------------------#

## FOR PROXY1_TYPE = MITEL

#PROXY1_ADDR     = 172.29.102.160:5060      # replace the ip address with your PBX's Address
#PROXY1_KEYPRESS_2833 = enable
#PROXY1_KEYPRESS_INFO = disable
#PROXY1_HOLD_IP0 = enable
#PROXY1_PRACK = enable
#PROXY1_REREG_SECS=3600
#PROXY1_KEEPALIVE_SECS=14
#PROXY1_DOMAIN =                            # Put Your SIP Domain's Name Here
#PROXY1_CALLID_PER_LINE = disable
#PROXY1_MAIL_ACCESS = 7000                  # Put Your Voice Mail Sytem's Pilot Number here

#-------------------------------------------------------------------------------------------#

## FOR PROXY1_TYPE = CCME

#PROXY1_ADDR     = 172.24.144.107:5060      # replace the ip address with the UCME's Address
#PROXY1_KEYPRESS_2833 = disable
#PROXY1_KEYPRESS_INFO = enable
#PROXY1_HOLD_IP0 = enable
#PROXY1_PRACK = enable
#PROXY1_REREG_SECS=3600
#PROXY1_KEEPALIVE_SECS=14
#PROXY1_DOMAIN =                            # Put Your SIP Domain's Name Here
#PROXY1_CALLID_PER_LINE = enable
#PROXY1_MAIL_ACCESS = 7999                  # Put Your Voice Mail Sytem's Pilot Number here

#-------------------------------------------------------------------------------------------#

## FOR PROXY1_TYPE = PINGTEL

#PROXY1_ADDR     = 172.24.144.127:5060      # replace the ip address with the Pingtel's Address
#PROXY1_KEYPRESS_2833 = enable
```

```
#PROXY1_KEYPRESS_INFO = disable
#PROXY1_HOLD_IP0 = enable
#PROXY1_PRACK = enable
#PROXY1_REREG_SECS=3600
#PROXY1_KEEPALIVE_SECS=14
#PROXY1_DOMAIN = asia.polycom.com            # Put Your SIP Domain's Name Here
#PROXY1_CALLID_PER_LINE = disable
#PROXY1_MAIL_ACCESS = 101                    # Put Your Voice Mail Sytem's Pilot Number here

#-------------------------------------------------------------------------------------------#

## FOR PROXY1_TYPE = ININ

#PROXY1_ADDR     = 172.24.144.135:8060       # replace the ip address with the II's Address and
port number
#PROXY1_FAILOVERIP = 172.24.144.136:8060     # replace the ip address with the secondary ININ IP
address.
#PROXY1_KEYPRESS_2833 = enable
#PROXY1_KEYPRESS_INFO = disable
#PROXY1_HOLD_IP0 = enable
#PROXY1_PRACK = enable
#PROXY1_REREG_SECS=3600
#PROXY1_KEEPALIVE_SECS=14
#PROXY1_DOMAIN =                             # Put Your SIP Domain's Name Here
#PROXY1_CALLID_PER_LINE = disable
#PROXY1_MAIL_ACCESS = 7999                   # Put Your Voice Mail Sytem's Pilot Number here

#-------------------------------------------------------------------------------------------#

## FOR PROXY1_TYPE = TOSHIBA

#PROXY1_ADDR     = 172.29.102.106:5060       # replace the ip address with the CIX100's Address
#PROXY1_KEYPRESS_2833 = enable
#PROXY1_KEYPRESS_INFO = disable
#PROXY1_HOLD_IP0 = enable
#PROXY1_PRACK = enable
#PROXY1_REREG_SECS=3600
#PROXY1_KEEPALIVE_SECS=14
#PROXY1_DOMAIN =                             # Put Your SIP Domain's Name Here
#PROXY1_CALLID_PER_LINE = disable
#PROXY1_MAIL_ACCESS = 290                    # Put Your Voice Mail Sytem's Pilot Number here

#-------------------------------------------------------------------------------------------#

## FOR PROXY1_TYPE = CCM

#PROXY1_ADDR     = 172.24.144.103:5060       # replace the ip address with the CCM's Address
#PROXY1_KEYPRESS_2833 = enable
#PROXY1_KEYPRESS_INFO = disable
#PROXY1_HOLD_IP0 = enable
#PROXY1_PRACK = enable
#PROXY1_REREG_SECS=3600
#PROXY1_KEEPALIVE_SECS=14
#PROXY1_DOMAIN =                             # Put Your SIP Domain's Name Here
#PROXY1_CALLID_PER_LINE = enable
#PROXY1_MAIL_ACCESS = 9999                   # Put Your Voice Mail Sytem's Pilot Number here

#-------------------------------------------------------------------------------------------#

## FOR PROXY1_TYPE = 3COM

#PROXY1_ADDR     = 172.29.102.190:5060       # replace the ip address with the 3COM's Address
#PROXY1_KEYPRESS_2833 = enable
#PROXY1_KEYPRESS_INFO = disable
#PROXY1_HOLD_IP0 = enable
```

```
#PROXY1_PRACK = enable
#PROXY1_REREG_SECS=3600
#PROXY1_KEEPALIVE_SECS=14
#PROXY1_DOMAIN =                              # Put Your SIP Domain's Name Here
#PROXY1_CALLID_PER_LINE = disable
#PROXY1_MAIL_ACCESS = 5000                    # Put Your Voice Mail Sytem's Pilot Number here

#-------------------------------------------------------------------------------------------#
## FOR PROXY1_TYPE = DELTAPATH

#PROXY1_ADDR     = 10.240.240.226:5060       # replace the ip address with the Asterisk Server's
Address
#PROXY1_KEYPRESS_2833 = enable
#PROXY1_KEYPRESS_INFO = disable
#PROXY1_HOLD_IP0 = disable
#PROXY1_PRACK = enable
#PROXY1_REREG_SECS=3600
#PROXY1_KEEPALIVE_SECS=14
#PROXY1_DOMAIN = axlx.engr.local             # Replace this with your SIP Domain's name
#PROXY1_CALLID_PER_LINE = disable
#PROXY1_MAIL_ACCESS = 7999                   # Put Your Voice Mail Sytem's Pilot Number here

#-------------------------------------------------------------------------------------------#
## FOR PROXY1_TYPE = SHORETEL

#PROXY1_ADDR     = 172.29.102.212:5060       # replace the ip address with the Shoretel's Address
#PROXY1_KEYPRESS_2833 = enable
#PROXY1_KEYPRESS_INFO = disable
#PROXY1_HOLD_IP0 = disable
#PROXY1_PRACK = enable
#PROXY1_REREG_SECS=3600
#PROXY1_KEEPALIVE_SECS=14
#PROXY1_DOMAIN = asia.polycom.com            # Put Your SIP Domain's Name Here
#PROXY1_CALLID_PER_LINE = disable
#PROXY1_MAIL_ACCESS = 102                    # Put Your Voice Mail Sytem's Pilot Number here

###############################################################################################
##### THIS SECTION EXPLAINS THE PROXY_N PARAMETERS IN MORE DETAIL AND GIVES FORMAT EXAMPLES ####

# One PROXYn_ADDR (PBX/Call Server) entry is required, additional ones are optional as you
#  can register secondary line appearances with other PROXY servers
#
#PROXY1_ADDR     = 172.29.102.131:5060
#PROXY2_ADDR     = 172.29.0.140:5060

#-------------------------------------------------------------------------------------------#


# For each proxy of type NECSIP, one PROXYn_CONF_IP_ADDRESS is required. This value is
# the address of NEC PBX's IP PAD card.
#
#PROXY1_CONF_IP_ADDRESS       = 172.29.102.131

#-------------------------------------------------------------------------------------------#



# To test ININ Redundancy PROXY1_FAILOVERIP is required. This value is the secondary IP address
# of the ININ server. If the primary server fails we need to use this address to make the calls.
#
#PROXY1_FAILOVERIP = 172.24.144.136

#-------------------------------------------------------------------------------------------#

#ProxyDomain can be omitted if a specific proxy domain name is not defined at the
```

```
# proxy server. If omitted, the ProxyDomain defaults to the IP address of the
# proxy server.
# (below are examples of different ways to specify a domain)
#PROXY1_DOMAIN = plcmengr.com
#PROXY1_DOMAIN = 10.0.0.138
#PROXY1_DOMAIN = axlx.engr.local

#-------------------------------------------------------------------------------------------------#


# PROXYn_MAIL_SUBSCR is who we should subscribe to for mail center notifications
# This is needed only if the user is not subscribed automatically at registration.
# It is almost never required in current versions of Asterisk to specify this.
# If you are using Asterisk (non-business edition) before v1.2, this is necessary.
# This example is actually specific for a line number:3001
#PROXY1_MAIL_SUBSCR = sip:3001@vmail.asterisk.com

#-------------------------------------------------------------------------------------------------#

# PROXYn_MAIL_ACCESS is the main voicemail dial number
# Examples:
#PROXY1_MAIL_ACCESS = 7999
# PROXY1_MAIL_ACCESS = sip:7999@10.0.0.138
# PROXY1_MAIL_ACCESS = 7999@10.0.0.138
# PROXY1_MAIL_ACCESS = 7999

#-------------------------------------------------------------------------------------------------#

#PROXYn_KEYPRESS_2833 controls generation of in-stream RFC2833 formatted key
# press events. Normally you want this to be disabled for Asterisk but it depends
# on your configuration and what you want to be able to do.
# If you are going to do OAI integration, this must be disabled.
# The default is disable
#PROXY1_KEYPRESS_2833 = disable

#-------------------------------------------------------------------------------------------------#

#PROXYn_KEYPRESS_INFO controls generation of SIP INFO requests to the SIP server
# for keypress events.  Normally you want this to be enabled.
# If you are going to do OAI integration, this must be enabled.
# The default is enable
#PROXY1_KEYPRESS_INFO = enable

#-------------------------------------------------------------------------------------------------#

# PROXYn_HOLD_IP0 controls setting of media stream IP destination to 0.0.0.0 when
# a call is put on hold.
# PROXYn_HOLD_IP0 is not required for current versions of Asterisk.
#  For older PBXs that require this, set this to enable
# Try toggling this value if you are having problems with hold
#PROXYn_HOLD_IP0 = enable

#-------------------------------------------------------------------------------------------------#

# PROXYn_PRACK enables ACK'd provisional responses to INVITE requests.  The PRACK
#  mechanism will be used if this switch is enabled and the Proxy server specifies
#  support for the PRACK mechanism.  PRACK is NOT SUPPORTED in current versions of
#  Asterisk, but is to be supported on subsequent versions.  PRACK should not be
#  required on local area networks.
#PROXY1_PRACK = disable

#-------------------------------------------------------------------------------------------------#


# PROXYn_KEEPALIVE_SECS specifies that the phone should send Keep Alives to the
```

```
#  PROXYn server.  It can be set to 0 or anywhere from 10 to 3600 seconds.
#  The default value (which is applied if no parameter is supplied in this file) is
#  0 which means the phone will not send keep_alives to PROXYn.
#
#  If the phone failes to get a keepalive response within the SIP 32 second
#  timeout, the keepalives are terminated for that PROXY until the next successful
#  registration to the PROXY.
#
#  This parameter is REQUIRED on Asterisk Business Edition with the Polycom 8002
#  phone. For Polycom 8020/8030 phones, this parameter is required when they are
#  operating in WI-FI standard QoS mode.This is because Linux, the OS running Asterisk,
#  has a ARP Cache flushing mechanism. This feature serves to refresh the ARP Cache for the 8002
phones.
#  For 8020 and 8030 phones, operating in SVP mode ARP Cache is refreshed by the SVP server.
#  If the phones are operating in standard based QoS method ARP cache refresh has to be done by
phone.
#
#  The value of this parameter for phones should be just less than the
#  minimum ARP Cache flushing time on the Linux box running Asterisk.  For Redhat
#  this minimum flushing time is 15 seconds, so the parameter needs to be set for
#  14 seconds or less.  For other Linux Distributions, you may have to determine
#  what this minimum value is, however 14 seconds should work fine.
#
#  The lower this setting, the more the impact on the phone's standby battery life.
#  (8002 phones running version 130.003 and earlier code ignore this parameter if
#  present)
#  8020/8030 phones running version 131.017 and earlier code ignore this parameter if
#  present)
#PROXY1_KEEPALIVE_SECS=14

#-------------------------------------------------------------------------------------------#

# PROXYn_REREG_SECS specifies the the re-registration interval for a PROXY.  This
#  is the requested expiration interval sent in the REGISTER request message.  It can
#  be set to anything between 35 and 3600 seconds.
#  The default value (which is applied if no parameter is supplied in this file) is
#  3600 which means the phone will attempt to register every 3580 seconds, if the
#  server's response interval doesn't take precedence (see below).
#
#  If the server has a lower maximum setting or a higher minimum setting that
#  this value then the server's response will take precedence and this parameter
#  will be ignored.
#
#  The phone will always attempt to re-register with the PROXY 20 seconds prior to
#  the expiration interval.  Thus, if this parameter is set to 35 seconds, and the
#  server's response interval doesn't take precedence, then the phone will attempt
#  to re-register every 15 seconds.
#
#  The lower this setting, the more the impact on the 8002's standby battery life.
#(8002 phones running version 130.003 and earlier code ignore this parameter if
# present)
#PROXY1_REREG_SECS=3600

#-------------------------------------------------------------------------------------------#

# PROXYn_CALLID_PER_LINE controls sending of same Call-ID header
# field for registrations sent to a particular registrar."
# If this is enable we will send  Call-ID headers differently.
# This may be needed for Mitel 3300 Controller software prior to Release 9
#PROXYn_CALLID_PER_LINE = enable

#-------------------------------------------------------------------------------------------#

# PROXY1_MAIL_SUBSCR is who we should subscribe to for mail center notifications
# This is needed only if the user is not subscribed automatically at registration.
```

```
# It is almost never required in current versions of Asterisk to specify this.
# Mitel, Cisco, Interactive Intelligence, and Pingtel also accept this parameter
# If you are using Asterisk (non-business edition) before v1.2, this is necessary.
# This example is specific for a line number:3001
#PROXY1_MAIL_SUBSCR = sip:3001@172.29.102.160
#PROXY1_MAIL_SUBSCR = sip:3001@yourdomain.name.here




# ////////////////////////////////////////////////////////////////////////////////////////////#
#  //////  The administrator should enter the extension specific configuration
#  //////  parameters for this extension in this section of the file
#  ////////////////////////////////////////////////////////////////////////////////////////////#


# Authentication credentials (Normally not stored in this file for security reasons)
# AUTH = username; password
# For lines on proxies of type NECSIP and SHORETEL, the LINEn_AUTH setting should be used instead
#  as each NEC line must respond to any authentication challenge using a single UN/PW pair.
#AUTH = 3001; 3001
# ////// For CCME, the value for LINEn_CALLID cannot have commas or special characters.
# ////// If a comma or a special character is in this command, phone will display an
# ////// error message "Bad Request 'Mal".
#--------------------------------------------------------------------------------------------#

# Line definitions
#  Each definition should have LINEn, LINEn_PROXY and LINEn_CALLID
#  LINEn is the dial number
#  LINEn_PROXY is the PROXYn server this line should register with, typically
#   defined in sip_allusers.cfg.
#  LINEn_CALLID is shown on the standby display of 8020/8030 phones but not 8002
#   or e/h340/i640 phones.  The Asterisk Server converts the callID information
#   to alternative forms defined in the Asterisk configuration files for
#   display at the far end of a phone call.
#  LINEn_AUTH is a means of associating a particular user-name/Password pair with a specific
line.
#  Linen_AUTH method of authentication must be used on PROXY types; NEC and SHORETEL
#   Like AUTH, there is a security risk associated with storing authentication credentials in
this file.
#   alternatively, the LINEn_AUTH setting information can be administered via the SIP Reg menus.
#  Up to 5 line definitions can be made for each user
#  Line definitions do not necessarily have to have different extensions

# ////// For CCME, the value for LINEn_CALLID shouldn't have commas or special characters.
# ////// If found, the phone will display an error message "Bad Request 'Mal".

LINE1         = 3001
LINE1_PROXY   = 1
LINE1_CALLID  = User Name 1
LINE1_AUTH    = 3001; 3001

# Two lines may map to the same extension to allow second incoming calls.
LINE2         = 3002
LINE2_PROXY   = 1
LINE2_CALLID  = User Name 2
LINE2_AUTH    = 3002; 3002

LINE3         = 3003
LINE3_PROXY   = 1
LINE3_CALLID  = User Name 3
LINE3_AUTH    = 3003; 3003

#LINE4         = 3004
```

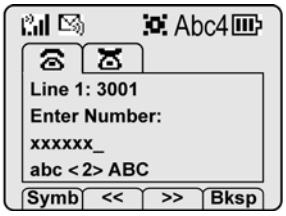
```
#LINE4_PROXY   = 3
#LINE4_CALLID  = User Name 4
#LINE4_AUTH    = 3004; 3004

#LINE5         = 3005
#LINE5_PROXY   = 2
#LINE5_CALLID  = User Name 5
#LINE5_AUTH    = 3005; 3005


##############################################################################
##### This section describes how to add Favorites ############################

#  Favorite Dialed Number list.
#   You can define up to 15 total entries including any defined in sip_allusers.cfg.
#   You can enclose a string in quotes to allow for spaces.
#   Each favorite can be complete SIP URI
#   Format is:
#       FAVORITE = dial_string; username
#
#    The username can be blank and can include escaped chars.
FAVORITE = 3001; User Name 1
#FAVORITE = 3002; User Name 2
#FAVORITE = 3003; User Name 3
#FAVORITE = 3004; User Name 4
#FAVORITE = 93035551212; User Name 5 Cell
#FAVORITE = 3006; User Name 6
#FAVORITE = 3007; User Name 7
#FAVORITE = 3008; User Name 8
#FAVORITE = 3009; User Name 9
#FAVORITE = 3010; User Name 10
#FAVORITE = 3011; User Name 11
#FAVORITE = 3013; User Name 12
#FAVORITE = 3013; User Name 13
#FAVORITE = 3014; User Name 14
#FAVORITE = 3015; User Name 15
#
#   Favorites can also be configured to prompt users to enter more digits. Users will
#   be prompted with characters inside the <>'s.
#   In the below example if the Feature Access Code for call forwarding is #21
#   When the user selects the Favorites option and then Call Forward they would
#   see "Call Forward Enter Destination:"
#   They would then have a chance to enter the fwd destination before pressing the send key
#FAVORITE =  #21<Enter Destination:>; "Call Forward"
#   In the example below the user would be prompted "Call Pickup Pickup Number:
#   to enter a call pickup number # for a call pickup Feature Access Code starting with *5
#FAVORITE =  *5<Pickup Number:>; "Call Pickup"
```

6

Using the SIP Handset

The Handset Display

When active, the handset screen will display either a call status screen or one of several menu screens. The call status screen has the following format:



This example shows two call tabs indicating that two calls are in progress. The un-selected call tab indicates that we have put another call on hold. The call-status icon for the selected call indicates that this call is being dialed. The text indicates the selected call is on line 1, extension 3001. Enter Number indicates that the handset is ready to be dialed. Once this call is connected, the connected party's information will appear on the third line, and the fourth line contains help or error messages, as appropriate. The softkeys during this action offer text editing functions.

System icons

Indicator	Function
	The signal-strength icon indicates the strength of the signal and can assist the user in determining if the handset is moving out-of-range.
	The voicemail icon is activated when a new voicemail message is received if the feature is supported by the phone emulation.
	The battery icon indicates the amount of charge remaining in the Battery Pack. When only one level remains, the Battery Pack needs to be charged.
	The speakerphone icon displays when the speakerphone is active.

Indicator	Function
◆▲▼▶	Up and down arrows are displayed when the menu has additional options above or below. Left or right arrows are displayed during editing when the cursor may be moved left or right.
	The Push-to-talk (PTT) ring icon. A PTT call is coming in.
	The priority PTT ring icon. A call is coming in on the priority PTT channel. This call will override any other.
	Location Service icon: indicates the Ekahau Real-Time Location System (RTLS) is enabled.
Locked	Locked indicates that the keypad is locked to prevent accidental activation. Use the **Unlk** softkey plus the **#** key to unlock it.
[No Service message]	If warning tones are not disabled, an alarm will sound and a descriptive message displays when the handset cannot receive or place calls. You may be outside of the covered area. Walk back into the covered area. The in-service tone indicates service is reestablished.
	The download icon indicates that the handset is downloading code. This icon only appears while the handset is running the over-the-air downloader. It appears to the right of the Signal Strength icon in the same location as the Voicemail icon.
XXXX	During character entry, Indicates current data entry symbol mode.

Call status icons

Indicator	Function
	On-hook icon, Solid when in standby mode to indicate that at least one call is still active or on hold. Flashing when incoming call is ringing.
	Off-hook icon. Solid when a call is being dialed.
	Hold icon. Call is on hold
	Transfer icon. Call is in the process of being transferred
	Audio flowing icon. Audio is flowing both ways on a call.
	Audio receive-only icon. Locally muted (flash) or far end hold with no music on hold.
	No audio icon. No audio is flowing. Call is terminating or far end hold with audio disable.

NavOK functions

The **NavOK** key acts as a fifth softkey with implicit functionality as follows:

State	NavOK key function
Dialing	Place phone call.
Answering	Answer a second phone call (same or different line)
Holding	Resume audio.
Displaying menu	Select the highlighted menu option.
Displaying call status	Resume audio on the currently selected call and place previous call on hold. If the selected call is ringing, the call will be answered.
Entering login name or login password	Save name or password and proceed with startup.

Softkeys

Softkey	Name	Displayed during…	Press to…
<<	Cursor backward	Entering a dial number.	Move the cursor back one position.
>>	Cursor forward	Entering a dial number.	Move the cursor forward in alphanumeric mode, if the cursor is at the end of the line, adds a space character.
Answ	Answer	Incoming call on the selected line.	Answer the call (equivalent to **START** key).
Bksp	Backspace character	Entering a dial number.	Delete the character prior to the cursor position.
Back	Back one screen	Displaying a menu.	Exit the menu.
Dial	Dial Call	A dial number is being entered on the selected line.	Initiate a phone call to the entered dial number.
End	End Call	An active call on the selected line.	Terminate the call without going back to standby mode.
Favr	Favorites	Prior to entering the first character of a dial number	Activate the Favorites menu.
Fwd	Forward Definition	Prior to entering the first character of a dial number.	Delete a previously defined forward destination. Or initiate definition of a new forward destination.

Softkey	Name	Displayed during…	Press to…
Hold	Hold	In an active call.	Place the call on hold. The line status shows when the call is on hold or when audio is flowing.
Msg	Message	Initial dial screen when new line is selected and a dial tone is active prior to entering first character of the number to be dialed[7].	Initiate a call to the specified message center contact address for retrieval or administration of voicemail.
Mute	Toggle muting	In an active call.	Toggle audio transmission to the far end. The line status shows when not muted or when muted.
OK	OK	Power up registration if username is not configured in **Admin** menu.	Send the username and password to the SIP server for authorization to register the handset.
Redl	Redial	Prior to entering the first character of a dial number.	Redial the last number that was dialed.
Rej	Reject	Incoming call on the selected line.	Reject the incoming call. The SIP server will then redirect the call elsewhere.
Resm	Resume	In an active call and you have placed the call on hold or in standby mode if any call is on hold.	Resume a call that was previously placed on hold or that went on hold when another line was activated.
Save	Save	Entering a dial number as a forward destination.	Save the dial number as the forwarding destination for the selected line.
Symb	Symbols	Entering a username or password. Entering the digits of a number.	Select the set of symbols available on the keypad while entering data.

[7] Appears only if the PROXYn_MAIL_NOTIFY is configured. A message center contact address must be defined for the proxy used by the selected line.

Menus

Line menu

The Line menu allows you to activate a call on a selected line or to view the status of lines.

Pressing the **LINE** key from the active mode displays a menu of line appearances as programmed in the SIP TFTP configuration file. The **LINE** key can be pressed while the handset is in the standby mode to activate the handset and to activate a new call on the selected line.

The currently selected line is indicated by an asterisk (*). Lines for which the corresponding proxy server has outstanding new mail are flagged with plus (+) characters. Lines that should be registered to a proxy but have failed registration for any reason are displayed in faded text and are not selectable from the menu.

Exit the **LINE** display by pressing a line number key to start a new call on the selected line and put any other call on hold, or by pressing the **END** key to exit without starting a new call. Press the **More** softkey to page through additional items on the Line menu.

Symbol menu

The symbol menu allows you to change the set of characters available for data entry through multiple key presses of the dial pad keys.

While dialing a number or entering login information, press the **Symb** softkey to view a menu of possible sets of characters that can be entered using multiple key presses of the dial pad keys. Normally, a simple numeric mode is selected; selecting other symbol modes allows convenient access to the complete printable US ASCII character set. The following table shows what characters are available through repeated key presses in various symbol modes.

Key	Number	English	Number + English	Punctuation
1	1	1 ; : / \ ! ‘	1	@ : 1
2	2	a b c 2 A B C	2 A B C a b c	; , 2
3	3	d e f 3 D E F	3 D E F d e f	& | ` ~ 3
4	4	g h I 4 G H I	4 G H I g h i	( ) 4
5	5	j k l 5 J K L	5 J K L j k l	< > 5
6	6	m n o 6 M N O	6 M N O m n o	{ } 6

Key	Number	English	Number + English	Punctuation
7	7	p q r s 7 P Q R S	7 P Q R S p q r s	[ ] 7
8	8	t u v 8 T U V	8 T U V t u v	‘ “ \ 8
9	9	w x y z 9 W X Y Z	9 W X Y Z w x y z	^ _ 9
0	0	@ - _ 0 = , < >	0 - _	[space] 0
*	. *	. $ * & % + ( )	* .	* . = + / -
#	@ *	[space] , ( ) |	# [space]	# ! ? $ %

Favorites menu

The Favorites menu assists you in dialing by providing access to a predefined list of dial numbers. The predefined list can include either complete dial numbers for named parties or partial numbers that need additional data entry. This might be the case, for example, if a PBX feature access code for call forwarding is defined in the favorites list but you need to add the forwarding destination information before sending the call to the PBX to activate the feature.

While in a dialing state, press the **Favr** softkey to display a menu of pre-defined numbers or names that can be dialed (as programmed in the SIP TFTP configuration file.) When an item is selected from the list, the dial number is displayed. You may edit or add digits to the displayed number if necessary before pressing the **NavOK** key or **START** to place the call. When using the Favorites menu to perform a blind transfer to someone on the list, select an entry from the Favorites menu and then press **FCN** and select **Transfer.**

FCN menu

The FCN menu is accessible while in the active mode and provides these features:

Transfer

Do Not Disturb

Set/Clear Forward

<OAI>

<OAI>

<OAI>

Items on this menu are accessible through navigation and selection keys or through short-cut keys as displayed with the menu items. OAI functions are automatically added as items at the end of this menu when defined on an OAI server.

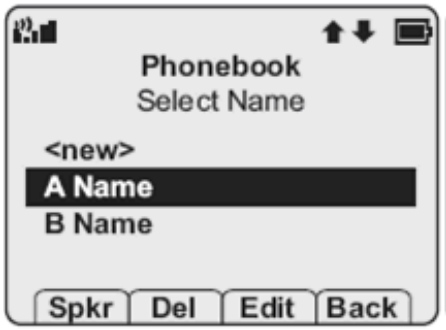
Handset Operation

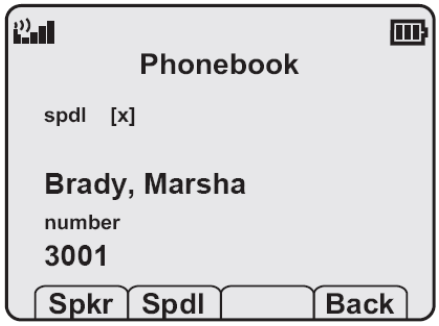
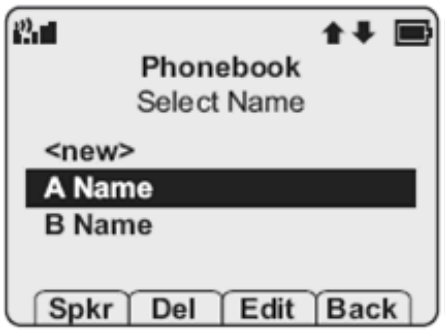
If you want to…	Then…
Turn the handset on	Press and hold the **END** key until two chirps sound.
Turn the handset off	Press and hold the **END** key. One chirp will sound. If you are in a call, hang up first, then turn off the handset.
Unlock the keypad	Press the **Unlk** softkey, then **#**.
Lock the keypad	While in Standby press the **Cfg** softkey, then press **NavOK**.
Place a call	1 To dial a number, follow any one of these sequences: » Press the **START** key, wait for a dial tone, then dial the number. Then press either **START** again or **Nav OK**. » Dial the number and then press the **START** key or **Nav OK**. » Press the **Spkr** softkey, then dial the number. Then press **START** or **Nav OK**. » Press the **START** key; press the **Favr** softkey; use the **Nav** ▲▼ keys to select the number or user from the list; press **Nav OK** to dial the number. 2 Listen for the ring to indicate the alerting of the called party. Note: **Line 1** is the default line.
Place a call from Favorites menu	1 Press **START** or **Spkr**. 2 Listen for dial tone. 3 Press the **FAVR** softkey. 4 Use the **Nav** keys to navigate to the desired entry. 5 Select the entry by pressing **NavOK**. 6 Press **START** or **NavOK** to place the call.

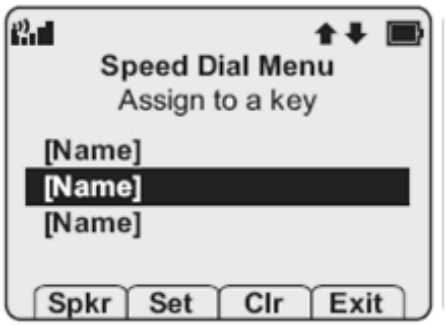
If you want to…	Then…
Place a second call	1 To get a dial tone for the second call, press **LINE** and **NavOK**. a. If the handset has multiple lines, press **LINE** + [the line number]. b. Press **NavOK**. • The first call is automatically placed on hold. • The second call appears in a new call tab. 2 Dial the number to place the second call. 3 Use the **Nav** ◄► keys to toggle between calls.
Place a call on a different line	1 Press the **LINE** key. 2 Navigate to the desired line and press **NavOK** or press the number of the line. 3 Dial the number. 4 Press **START** or **NavOK** to initiate the call.
Answer a call	• Press **START**, and hold the handset to your ear. • Press **NAV OK**, and hold the handset to your ear. • Press the **Answ** softkey and hold the handset to your ear. • Press the **Spkr** softkey and speak towards the handset.
Reject a call	Press the **Rej** softkey to reject the call and allow the SIP server to redirect the call elsewhere, usually to voicemail.
Answer a call on a second line	If another call comes in on a different line, a new call icon flashes and a tone sounds in the audio stream until the call is answered, the first call is terminated, the caller hangs up, or the call transfers to voicemail. 1 To view the caller ID of the incoming call without interrupting the active call, press **Nav** ►. The original call's audio remains active. The display now shows information about the incoming call. 2 Press **NavOK**, **START** or **Answ** to place the current call on **Hold** and answer the second call, or Press **Rej** to redirect the incoming call to voicemail or as otherwise programmed.
Navigate among call tabs	Use **Nav►** and **Nav◄**.

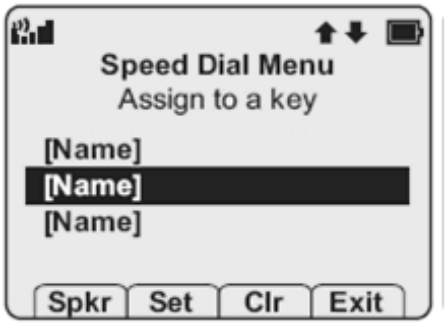
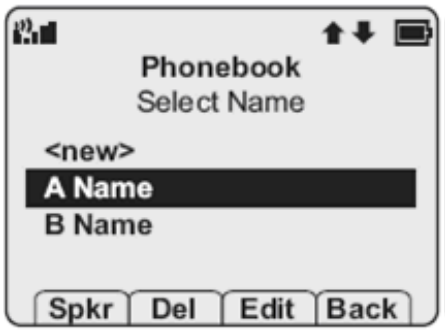
If you want to…	Then…
Forward calls	Calls may be forwarded on a per-line basis. The Line menu display will indicate if a line is forwarded by a **>** character followed by the destination address. • When a line is forwarded, the standby screen displays the forwarding status, unless the do-not-disturb feature is enabled. • If your handset has multiple lines, set or clear forwarding for each line individually. 1 Press **START** or press **Line** and a line number to select the line that you want to be forwarded. 2 Press **FCN** and select the **Set/Clear Forward** item from the **FCN** menu using a digit key or **NavOK** key. 3 Enter the forwarding number for the indicated line. 4 Press **NavOK** to save. To clear call forwarding for a given line #, again press **START** or select the line #. Again select the **Set/Clear Forward** item from the menu.
Clear forwarding on a line	Press **START** or select the line number. Select the **Set/Clear Forward** item from the menu.
Listen to voicemail	1 Press **START**. 2 Press **Msg** softkey, or Dial your voice message system number 3 Press **START** or **Nav OK**.
Do Not Disturb (reject all incoming calls)	1 Press **START**. 2 Press **FCN**. 3 Select the **Do-Not-Disturb** item from the menu and press **NavOK.** When the do-not-disturb feature is enabled, the standby screen will display **Do Not Disturb**. The handset will not ring for new incoming calls.
Clear Do Not Disturb	1 Press **START**. 2 Press **FCN**. 3 Select the **Do-Not-Disturb** item from the menu and press **NavOK** .
Redial the last number you dialed	1 Press **START**. 2 Press the **Redl** softkey. 3 Verify that the displayed number is the one you want and the line number is valid. 4 Press **NavOK** or **START**.

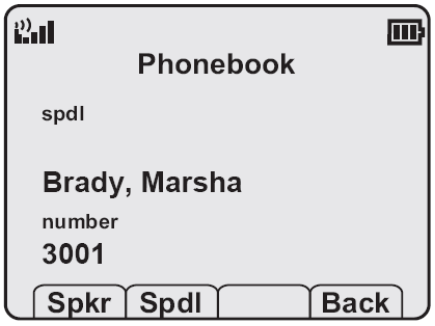
If you want to…	Then…
Activate installed custom applications (registered OAI application on an OAI server)	1 Press **START** or **Spkr**. 2 Press **FCN**. 3 Navigate to the desired custom application using **Nav** ▲▼ keys or the **More** softkey. 4 Select the application using **NavOK** or shortcut key.
Transfer a call (blind)	1 While in a call, press **FCN** and then select the transfer item by shortcut key or **NavOK**. (The current call will be placed on hold and it will be marked with a transfer icon ✕. A new call will be started and you will hear a dial tone.) 2 Dial the number to which you wish to transfer the call or press the **Favr** softkey and select an entry from the Favorites menu. 3 Press **FCN** and select the **Transfer** option again. The marked call will be transferred to the number that you have entered. 4 Press the **END** key to return to standby. If the transfer fails, you will see an error message and you can then pick up the original call by navigating to the marked call and pressing **NavOK**.
Transfer a call (consulted)	1 While in a call, press **FCN** and then select the transfer item by shortcut key or **NavOK**. (The current call will be placed on hold and it will be marked with a transfer icon ✕. A new call will be started and you will hear a dial tone.) 2 Dial the number to which you wish to transfer the call or press the **Favr** softkey and select an entry from the Favorites menu. 3 Press **NavOK** or **START** to establish a second call. 4 Inform the person on the other end that you would like to transfer the call. 5 Press **FCN** and select the **Transfer** option to transfer the call. 6 Press the **END** key to return to standby.
Transfer an active call to a call on Hold	1 Press **FCN** and then select the **Transfer** option by pressing **NavOK**. The current call will be placed on hold and it will be marked with a transfer icon ✕. 2 Navigate to the second call (already on hold). 3 Press the **Resm** softkey and tell the other party that the call will be transferred. 4 Press **FCN** and select the **Transfer** option by pressing **NavOK**. 5 Press the **END** key to return to standby.
Silence the ringing	Press the **END** key to silence the external speaker ring and convert to in-ear speaker ringing. External speaker ringing will resume when the next incoming call is received while the handset is in standby mode.

If you want to…	Then…
Change the ring volume	Press the up/down volume buttons on the side of the handset during ringing, or while the handset is in standby mode.
Adjust the speaker volume	While speakerphone is active, press the up/down volume buttons on the side of the handset during the call.
Adjust the headset volume	While the headset is plugged in, press the up/down volume buttons on the side of the handset during the call.
Mute/Unmute a call	Press the **Mute** softkey. When the handset is muted, the audio flowing icon ⇆ changes to the audio receive-only icon ⇇. Press the **Mute** softkey again to restore audio pickup.
End a call	Press the **End** softkey to maintain the active mode and view the active calls. Press the **END** key on the keypad to return to the standby mode.
Change the profile	Press the **Prof** softkey and use the **Nav** keys to select a new profile while in standby mode. The selected profile is marked with an asterisk (*****).
Open Config menu	Press the **Cfg** softkey from standby mode.
Turn on the backlight	The backlight comes on when any key is pressed or when there is an incoming call, and stays on for 10 seconds. It turns off if another key is not pressed within that period.
Resume a call on hold from standby.	Press the **Resm** softkey. If more than one call is on hold, use the **Nav** ◄ ► keys to select the call you wish to resume and press the **Resm** softkey or **NavOK**.
Open the phonebook	Press the **Phbk** softkey from standby mode. The phonebook may also be opened by pressing the **Save** softkey when it appears in a call log or during predialing.  The phonebook list is sorted alphabetically. The <**new**> option appears until the maximum number of entries (20) has been entered.

If you want to…	Then…
View system speed dial number	If the system speed dial key has been programmed, it will be listed as the first entry with a close bracket (>) as the first character. Only the system administrator may change this entry.
Search for a phonebook entry	Use Nav▲ and Nav▼ to scroll through the names or press the keys corresponding to the first letters of the name. Use Nav◄ and Nav► to edit the search characters as needed.
View a phonebook entry	Select the name and press **NavOK**.  The entry may be called, assigned a speed dial number or edited from this screen. If a speed dial number has been assigned to this name, it will appear beside **spdl**. Return to the phonebook list by pressing the **Back** softkey or **NavOK**.
Edit a phonebook entry	1 Select the name to edit from the phonebook list. 2 Press the **Edit** softkey to open the **Edit Number** display and edit the existing number. Use the Clr and Del softkeys as needed. 3 Press **NavOK** to display the **Edit Name** display and edit the name. 4 Press **NavOK** to save the changes and exit the editing screens. Press the **Back** softkey to exit without saving the changes.
Dial phonebook number	Select the entry and press **START** or the **Spkr** softkey. 

If you want to…	Then…
Enter a new name and number in the phonebook	1 Open the phonebook. 2 Select the <**new**> option (if available) and press the **Edit** softkey to open the **Enter Number** display. 3 Enter the name and number by following the steps for editing a name and number. You must enter alphanumeric characters for the name, not blank spaces.
Delete a phonebook entry	1 Open the phonebook and select the entry. 2 Press the **Del** softkey to delete the entry.
Open the speed dial list from standby	Press the **Spdl** softkey from standby mode. 
Make a speed dial call	1 From standby or while in the speed dial menu, press and hold the corresponding number key on the keypad for one second. The system speed dial key must be pressed for three seconds. 2 The handset will display the name and number for one second before the call is dialed. You may press **END** during this second to terminate the call. (You may also use the Nav keys to highlight an entry and then press **START** or the **Spkr** softkey to dial the number.) If you do not place a call, you may return to standby by pressing the Exit softkey.

If you want to…	Then…
Assign a speed dial number	A phonebook entry may be assigned to a speed dial key from the speed dial list or from the phonebook edit number display. From the speed dial list: 1 Select the speed dial key that you wish to assign.  2 Press the **Set** softkey to open the phonebook list. 3 Use the search routine or the **Nav** keys to select the desired entry.  4 Press **NavOK** to assign the selected name to that speed dial key. 5 Press **NavOK** again to exit to standby.

If you want to…	Then…
	From the phonebook view number display:  1 Press the **Spdl** softkey from the view number display in the phonebook. 2 When the speed dial list opens, navigate to an empty slot and press **NavOK**. This sets the speed dial key to the number in the phonebook. 3 Press **END** to exit to standby mode and save the speed dial number assignment. Speed dial entries may be edited through the phonebook, as described above.
Push to Talk	[the PTT Vibrate feature has been added]
PTT Vibrate	To enhance the alerting of a PTT call, **PTT Vibrate** may be enabled. When **PTT Vibrate** is enabled, the handset will vibrate three times whenever a PTT broadcast is received, whether the handset is in standby or in a call. If in a call, the chirp alert will also sound. The vibration does not replace any PTT tone volume already set. To set the handset for PTT vibrate only, enable **PTT Vibrate** and set the tone volume to zero. **PTT Vibrate** is disabled by default.
Emergency Dial	The large button on the left side of the SpectraLink 8030 Wireless Telephone may provide you with either Emergency Dial or PTT functionality as determined and activated by the system administrator. To determine if **Emergency Dial** has been activated, press this button one time. If **Emergency Dial** is active, an explanatory message will be displayed. When **Emergency Dial** has been enabled, the handset will dial an emergency number when it is pressed twice within two seconds. The number dialed may be found under the **Config Menu**>**System Info** option. Note that this feature is functional when the keypad is locked.
	Caution! Emergency Dial will be inoperable if the wireless system or the call server fails for any reason. Do not rely on it as the sole method of emergency notification.

7

Testing a Handset

Verify proper registration and operation of each handset by performing the following tests on each handset in an active wireless area.

1. Power on the handset by pressing the **END** key. A series of messages will be displayed as the handset acquires the system. The handset should display the user extension.
2. Place a call and listen to the audio quality. End the call by pressing the **END** key.
3. Place a call to the handset and verify ring, answer, clear transmit, and clear receive audio.
4. Use the softkeys to verify all softkey programmed features on the handset.
5. Press the **END** key. Any line indicators should turn off and the extension number display will return.

If any of these steps fails to operate as described, refer to Chapter 11 *Troubleshooting* for corrective action.

8

Diagnostic Tools

Run Site Survey, **Diagnostics Enabled** and **Syslog Mode** are three diagnostic tools provided to assist the LAN administrator in evaluating the functioning of the SpectraLink 8020/8030 Wireless Telephone and the system surrounding it. Diagnostic Tools are enabled in the **Admin** menu.

The **Halt on Error** option in the Admin menu is a diagnostic tool that will cause the handset to stop operating if an error message is received. Error detail may be shown on the display, captured by the syslog server, and may also be available for downloading with the Handset Administration Tool. Unless the error is a fatal one, normal operation may be resumed by power-cycling the handset.

Run Site Survey

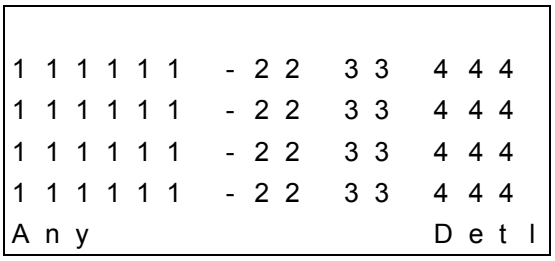
Site survey is used to evaluate the facility coverage before certifying that an installation is complete. It can also be used at any time to evaluate coverage by testing signal strength, to gain information about an AP, and to scan an area to look for all APs regardless of SSID. The information available through the site survey includes:

- SSID
- Beacon Interval
- AP information regarding support of 802.11d, 802.11h and other 802.11 amendment standards as required
- Current security configuration

Start the site survey by selecting **Run Site Survey** from the **Admin** menu. The mode starts immediately.

When the test is started, it is by default in "single SSID" mode. When the **Any** soft key is pressed (softkey A) all APs, regardless of SSID, are displayed and the softkey changes to say **MyID**. Pressing the **MyID** soft key will revert to the "single SSID" mode and change the softkey back to **Any**.

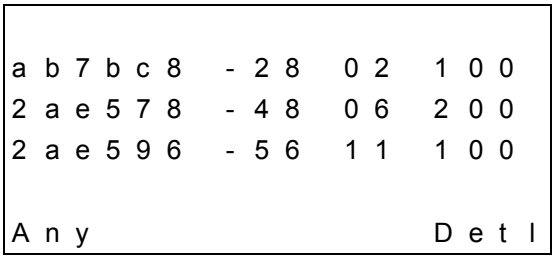
The display would look like the following for the single AP mode.



Where:

- 111111 – the last three octets of the on-air MAC address for a discovered AP.
- 22 – the signal strength for the specified AP.
- 33 – the channel number of the specified AP.
- 444 – the beacon interval configured on the specified AP.
- Any/MyID – softkey to toggle between "single SSID" and "any SSID" mode.
- Detl/Smry – softkey to toggle between the multiple AP (summary) display, and the single (detail) displays for each AP.

The following screen shows how the display would look when there are three APs configured with an SSID that matches that of the handset. The first has a signal strength of –28 dBm, is configured on channel 2, with a beacon interval of 100 ms. The second has a signal strength of –48 dBm, is configured on channel 6, with a beacon interval of 200 ms. The third has a signal strength of –56 dBm, is configured on channel 11 with a beacon interval of 100 ms.



When the **Any** SSID mode is selected, the summary display contains the first six characters of the APs SSID instead of the beacon interval as in the example below.

```
a b 7 b   - 2 8   0 2   A L P H A
2 a e 5   - 4 8   0 6   W S M T E S
2 a e 5   - 5 6   1 1   v o i c e

M y I D                 D e t l
```

In **Detl** (detail) mode the display would appear as follows. The left/right arrow keys will move between AP indices.

```
i : b b b b b b   s n   c h   b c n
e e e e e e e e e e   D G H I
r r r r r r r r r r r r + x x x x
Q : X P   C : v C   s s s s s s s
A n y                   S m r y
```

Where:

- i – index of selected AP (value will be from 0 to 3 inclusive)
- bbbbbb – the last three octets of the BSSID for a discovered AP
- sn – signal strength in –dBm
- ch – channel
- bcn – beacon interval
- eeeeeeeeeee – SSID (up to first 11 characters)
- DGHI – standards supported i.e. 802.11d, 802.11g, etc. in addition to 802.11a and 802.11b.
- rrrrrrrr – rates supported. Basic rates will have a "b" following the rate
- + – more rates are supported than those displayed
- xxxx – WMM or UPSD if those QoS methods are supported
- Q:XP
    - X is a hexadecimal representation of the access categories configured with admission control mandatory (ACM). Bit3 = voice, Bit2 = video, Bit1 = background, Bit0 = best effort. For example, if an AP advertises voice and video as ACM then X=c. If all the ACs are set as ACM then X=f. If

AP does not have WMM support, this character space will be blank.

  - P is displayed when the AP advertises WMM-PS. If the AP does not advertise WMM-PS then this character space will be blank.

- C:vC
  - v is a decimal number indicating the CCX version advertised by the AP.
  - C is displayed when AP advertises CCKM. If the AP does not advertise CCKM then this character space will be blank.
- sssssss – Security modes: “None”, “WEP”, “WPA-PSK”, “WPA2-PSK”, “WPA2-Ent”
- Any/MyID – softkey to toggle between “single SSID” and “any SSID” modes
- Detl/Smry – softkey to toggle between the multiple AP display (summary), and the single AP display (detail)

Numbers racing across the handset display indicate AP information is being obtained. A **Waiting** message indicates the system is not configured properly and the handset cannot find any APs.

Solving coverage issues

Coverage issues are best resolved by adding and/or relocating APs.

Overlap issues may be resolved by reassigning channels to the APs or by relocating them. See Chapter 11 *Troubleshooting*, section *Access Point Problems* for more information.

Diagnostics Enabled

Diagnostics is used to evaluate the overall quality of the link between the handset, AP, and infrastructure side equipment, such as IP PBX, SpectraLink 8000 SVP Server, and gateways. Unlike **Site Survey**, **Diagnostics** is used while the functional code is running, and during a call.

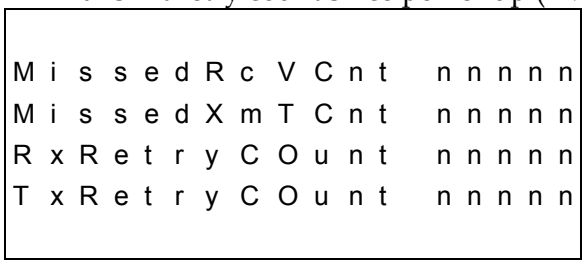
When **Diagnostics** is enabled in the **Admin** menu, the handset can display diagnostic screens any time it is in active mode.

The display of information is instigated, when in call, by pressing the **Nav**◄ or **Nav**► key. Only one of the six diagnostic screens listed below can be shown at a time. Pressing the **Nav** keys multiple times will cycle through the various diagnostics screens and the normal off-hook (IP-PBX) display. The numeric icon at the top of the display indicates what screen number is being displayed. For example: The first time the **Nav** key is pressed, the **1** icon is shown, and the first of six diagnostics screens are displayed. The next time it is pressed, the **2** icon is shown, and the next of six diagnostics screens are displayed. The counters will be cycled through in this fashion until there are no more counters to be displayed. After all the diagnostics screens have been displayed, the screen returns to the normal off-hook IP-PBX screen.

The information provided by **Diagnostics** includes:

Screen 1

- Missed receive packet count since power up (MissedRcvCnt)
- Missed transmit packet count since power up (MissedXmtCnt)
- Receive retry count since power up (RxRetryCount)
- Transmit retry count since power up (TxRetryCount)



Screen 2

- Jitter – average error or "wobble" in received packet timing, in microseconds
- Last successful transmit data rate (LastRate)
- Gateway type (GatewyType)
- TX Power (dBm)

```
Jitter                  nnnnn
LastRate                mmmmm
GatewyTyPe              mnemo
TXPower(DBm)            rrrr
```

Where:

- nnnnn – Jitter in micro-seconds
- mmmmm – last transmit rate
  - 11Mb – SpectraLink System with SVP Server. Handsets can run at full 11Mb when in 802.11b/g mode
  - 54Mb – SpectraLink System with SVP Server. Handsets can run at full 54Mb when in 802.11a or 802/11g modes
- mnemo – a mnemonic that indicates what type of gateway is being used
- rrrrr – TX Power configured in dBm

Screen 3

Screen 3 contains a list of the APs that are heard and the following parameters from each AP:

- Indicator as to whether this is the current AP or an index into the list of other APs heard (C indicates current)
- Last 2 octets of the MAC address of the AP (mmmm)
- Channel number (ch)
- Signal strength (ss)
- Either the 802.11 Association ID from the current AP or a mnemonic for the reason code indicating why the handset didn't hand off to this other AP

```
mmmm   ch   -ss   aid
mmmm   ch   -ss   mnem
mmmm   ch   -ss   mnem
mmmm   ch   -ss   mnem
```

Where:

- mmmm – This hexadecimal number is the last 2 octets of this AP's MAC address
- ch – Channel number the AP is configured on
- -ss – Signal strength for the AP in dBm
- aid – The Association ID for the currently associated AP

AP mnem – a mnemonic indicating the reason code:

- Unkn – reason unknown
- Weak – signal strength too weak
- Rate – one or more basic rates not supported
- Full – AP can not handle bandwidth requirements
- AthT – authentication timeout
- AscT – association timeout
- AthF – authentication failure
- AscF – association failure
- SecT – security handshake timeout
- SecF – security handshake failure
- Cnfg – AP not configured correctly for security, QoS mode or infrastructure network
- CCX – AP is not CCX complaint.
- CCKM – AP does not support CCKM.
- WMM – AP does not meet the WMM requirements. Probable reason could be that the access categories AC_VO and AC_VI, used for voice and control traffic respectively, might not be marked as mandatory or WMM-PS might not be enabled.

Screen 4

- Association count since power up (AssocCount)

- Re-association count since power up (ReAssocCount)
- Association failures since power up (AssocFailure)
- Re-association failures since power up (ReAssocFail)

```
AssocCount          nnnnn
ReAssocCount        nnnnn
AssocFailure        nnnnn
ReAssocFail         nnnnn
```

Screen 5

- WEP only security error count since power up (Sec-ErrCount)
- MAC sequence number of frame with last security error (LstSecErrSeq)
- (Re)Association failures due to QoS (QoSFailCnt). Usually attributed to insufficient available bandwidth on an AP.

```
Sec-ErrCount        nnnnn
LstSecErrSeq        nnnnn
QoSFailCnt          nnnnn
```

Screen 6 – EAP Information

- "xxxxx" in Line 1 is a 5-digit decimal value displaying the EAP authentication failure/error count.
- "xxxxx" in Line 2 is a 5-digit decimal value displaying the error code/sequence for the last EAP authentication reason, listed just below. Line 2 will be blank if the count for Line 1 is zero.
- 1 = Unknown error
- 2 = Mismatch in EAP type. The phone is configured with an EAP type (Cisco FSR, PEAP or EAP-FAST) that is not supported by the AP.
- 3xxx = Certification failure. The certificate presented by the server is found as invalid. "xxx" when having a non-zero value, is the

standard TLS alert message code. For example, if a bad/invalid certificate (on the basis of its signature and/or content) is presented by the server "xxx" will be 042. If the exact reason for the certificate being invalid is not known, then the generic certificate error code would be xxx=000. [Refer http://www.ietf.org/rfc/rfc2246.txt , section 7.2 for further TLS alert/error codes].

- 4xxx = Other TLS failures. This is due to TLS failure other than certification related errors. The reason code (the TLS alert message code) is represented by "xxx". For example, if the protocol version presented by the server is not supported by the phone then xxx will be 70, and the EAP error code would be 4070. [Refer http://www.ietf.org/rfc/rfc2246.txt , section 7.2 for further TLS alert/error codes].

- 5xxx = Security credential Failure. This is due to an invalid username and/or password produced by the phone. xxx when non-zero, presented the 3-digit error code sent by the server in response to phone's credential. For example, if the server has sent the error code as "691", then the EAP error code would be 5691. If the server does not send the error code message, then xxx is defaulted to 000, i.e., EAP error code would be 5000. Refer [1]) http://www.ietf.org/rfc/rfc2759.txt section 6, [2] http://ietfreport.isoc.org/all-ids/draft-zhou-emu-fast-gtc-02.txt section 2.

```
EAP Err Cnt          xxxxx
Last EAP Er Code     xxxxx
```

Syslog Mode

A syslog server must be present on the network in order for the handset to send the log messages and have them saved. The syslog server will be found with DHCP option 7 if the handset is using DHCP. If static addresses are configured, the syslog server's IP address can be configured statically in the **Admin** menu.

If the syslog server address is blank (**000.000.000.000** or **255.255.255.255**) or the handset is using DHCP and no option 7 is received from the DHCP server, the handset will not send any syslog messages.

Admin menu options:

- ***Disabled** – turns syslog off.
- **Errors** – causes the handset to log only events that we consider to be an error (see below).
- **Events** – logs all errors plus some other interesting events (see below).
- **Full** – logs all the above plus a running stream of other quality information (see below).

The table below lists the syslog messages and which level of logging will produce them:

Message type	Errors	Events	Full
Failed Handoff	Yes	Yes	Yes
Successful Handoff	No	Yes	Yes
Security Error	Yes	Yes	Yes
Call Start/End	No	Yes	Yes
Audio stats	No	No	Yes (every 5 secs)
Audio error threshold exceeded	Yes	Yes	Yes
Radio stats	No	No	Yes (every 5 secs)
Radio error threshold exceeded	Yes	Yes	Yes
Error Handling Mode	Yes	Yes	Yes

All syslog messages will include:

- Date and time (to 1/100th of second) since handset power on (The handset time is set when it is powered on to Jan-1 00:00.00 GMT adjusted. If it has obtained a time from the network time server, that time will display instead.)
- Handset's MAC address
- Handset's IP address
- Sequence number

The table below lists the additional items in each message type:

Failed Handoff (Sent whenever the handset attempted to handoff, but failed trying.)	Failed AP MAC Failed AP signal strength Current AP MAC Current AP signal strength Failure reason Wireless Telephone Transmit Power to Old AP Wireless Telephone Transmit Power to New AP FCCKM‡ – Failed to use CCKM for fast handoff FOKC‡ – Failed to use OKC for fast handoff
Successful Handoff	New AP MAC New AP signal strength Old AP MAC Old AP signal strength Reason for handoff Other candidate APs: MAC Signal strength Reason not used Wireless Telephone Transmit Power to Old AP Wireless Telephone Transmit Power to New AP FCCKM‡ – Failed to use CCKM for fast handoff FOKC‡ – Failed to use OKC for fast handoff
Security Error	AP MAC AP signal strength Security mode Error details (mode-dependent)
Call Start	Call type (telephony, OAI, PTT) AP MAC AP signal strength

Call End	AP MAC AP signal strength
Audio stats	AP MAC AP signal strength Payload size (in msec) Payloads sent Payloads received Payloads missed (not received) Payloads missed rate (over last 5 seconds) Payloads late Payloads late rate (over last 5 seconds) Average jitter
Audio error threshold exceeded (Sent if payloads missed rate or payloads late rate exceeds 2%, or if the average jitter is over 2 msec)	Same as audio stats
Radio stats	AP MAC AP signal strength Directed packets sent Directed packets received Multicast packets sent Multicast packets received Broadcast packets sent Broadcast packets received TX dropped count TX drop rate (over last 5 seconds) TX retry count TX retry rate (over last 5 seconds) RX retry count RX retry rate (over last 5 seconds)
Radio error threshold exceeded (Sent if TX drop rate exceeds 2% or TX or RX retry rate exceeds 5%)	Same as radio stats
Probe Recovery	Probe Recovery Count
LockUpRecovery	Lockup Recovery Count
DCA initiated radio reset	Reset count when Reset occurred Reset count at the time when the syslog was sent

‡ Present only when the specific fast handoff method (CCKM, OKC) has been enabled.

Messages are formatted like the following example:

```
Jan 1 00:01:26.72 0090.7a02.2a1b (172.16.0.46) [001a]
RStat: AP 00:40:96:48:1D:0C (-56 dBm), Sent 783523,
Recvd 791342, MSnt 245, MRcd 5674, BSnt 43, BRcd 10783,
TX drop 43 (0.0%), TX retry 578 (1.2%), RX retry 1217
(1.6%)
```

9

Certifying the Handsets

Prior to determining that an installation is complete, test the handsets following the sequence given in the previous *Testing a Handset* section and conduct a **Site Survey** mode test according to the directions given in the previous *Diagnostic Tools* section.

The installation may need some adjustments. Note any areas where coverage is conflicting or inadequate. Note any system difficulties and work with your wireless LAN and/or LAN system administrator to determine the cause and possible remedy. See Chapter 11 *Troubleshooting* for clues to possible sources of difficulties. If any adjustments are made to the system, re-test the device in the same vicinity to determine if the difficulty is resolved.

The installer should not leave the site before performing installation verification.

These tests must be performed in typical operating conditions, especially if heavy loads occur. Testing sequence and procedure is different for every installation. Generally, you should organize the test according to area and volume, placing numerous calls to others who can listen while you perform coverage tests. Note any areas with excessive static or clarity problems and report it to a Polycom service engineer.

The coverage test will also require you to put the handset in **Site Survey** mode and walk the entire coverage area to verify all APs.

Conducting a Site Survey

Conduct a site survey of the installation, by walking the site looking for interfering 802.11 systems, adequate coverage and channel assignment, and correct AP configuration. The site survey discussed here does not replace an RF site survey conducted by professionals who specialize in WLAN design and voice optimization implementations. Polycom offers professional services including RF site surveys.

The handset's site survey mode is not a replacement for a professional site analysis and should be used only for testing, limited site validation, and troubleshooting.

The handset's site survey mode does not include functionality to allow for analysis or troubleshooting of 802.11n specific WLAN features.

1. Referring to Chapter 8 *Diagnostic Tools*, section *Run Site Survey*, put a handset into **Site Survey** in the **Any/Smry** ESSID mode. Walk throughout the site checking for any expected APs or other ESSIDs.
2. Then, walk the site again, in **MyID/Smry** ESSID mode, this time checking that every location has adequate coverage and has good channel allocation.

There should be at least one AP stronger than -the minimum specified in the following tables.

At any point, the strongest AP shown should be on a different channel than the next best choice.

The handset configured for 802.11b requires:

- -70dBm when all 802.11b data rates are available (with only 1Mbps set Required)
- -65dBm when only 2Mbps is set Required and other higher rates enabled
- -64dBm when only 5.5Mbps is set Required with 11Mbps set enabled
- -60dBm when 11Mbps is set required and other 802.11b rates disable or enabled

802.11 Radio Standard	Minimum Available Signal Strength (RSSI)	Maximum "Mandatory" Data Rate
802.11b	-70 dBm	1 Mb/s
	-60 dBm	11 Mb/s

- The critical factor is the highest data rate set Required or Mandatory. Other 802.11b data rates can be set enabled or disabled. The highest data rate set Required or Mandatory determines the RF power available to the wireless telephone for proper operation.

The handset configured for 802.11g requires:

- -60dBm when all 802.11g data are available (with only 6Mbps set Required)
- -45dBm when 54Mbps is set Required and other 802.11g rates Required, Enabled or Disable

802.11 Radio Standard	Minimum Available Signal Strength (RSSI)	Maximum "Mandatory" Data Rate
802.11g	-60 dBm	6 Mb/s
	-45 dBm	54 Mb/s

- The critical factor is the highest data rate set Required or Mandatory. Other 802.11g data rates can be set Required, Enabled or Disabled. The highest data rate set Required or Mandatory determines the RF power available to the wireless telephone for proper operation.
- -45dBm when 54Mbps is set Required and other 802.11g rates Required, Enabled or Disable

The handset configured for 802.11g requires:

- -60dBm when all 802.11a data are available (with only 6Mbps set Required)
- -45dBm when 54bps is set Required and other data rates Required, Enabled or Disabled

802.11 Radio Standard	Minimum Available Signal Strength (RSSI)	Maximum "Mandatory" Data Rate
802.11a	-60 dBm	6 Mb/s
	-45 dBm	54 Mb/s

- The critical factor is the highest data rate set Required or Mandatory. Other 802.11a data rates can be set enabled or disabled. The highest data rate set Required or Mandatory determines the RF power available to the wireless telephone for proper operation.

3. Finally, use the single AP (**MyID**/**Detl**) display to check each AP, to ensure it is configured for the proper data rates, beacon interval, 802.11 options enabled, QoS method, and security method.

Make any necessary adjustments to AP locations and configurations and repeat steps 1 through 3 until the site survey shows adequate coverage and correct configuration at every location.

The installation is not complete until these certification steps have been performed. Do not hand out handsets at a site that has not been certified.

10

Software Maintenance

The SpectraLink 8020/8030 Wireless Telephones use proprietary software programs written and maintained by Polycom Corporation. The software versions that are running on the handsets can be displayed during power on by holding down the **END** button. **Firmware Version** is also an option on the Config menu.

Polycom Customer Service or an authorized dealer will provide information about software updates and how to obtain the software (for example, downloading from a website).

After software updates are obtained, they must be transferred to the appropriate TFTP server located on the LAN to update the code used by the Wireless Telephone.

The handset allows over-the-air transfer of software updates from the designated TFTP server to the handsets. The download function in the Wireless Telephone checks its software version every time the handset is powered on, when the TFTP server is active. If there is a different version available, the handset immediately begins to download the update.

Upgrading Handsets

After software updates are obtained from Polycom, they must be transferred to the appropriate location in the LAN to update the code used by the handsets.

SpectraLink 8020/8030 Wireless Telephones allow over-the-air transfer of software updates from the designated TFTP server to the handsets. The downloader function in the handset checks its software version every time the handset is turned on. If there is any discrepancy the handset immediately begins to download the update.

Normal Download Messages

When the handset is powered on, it displays a series of messages indicating that it is searching for new software, checking the versions, and downloading. The normal message progression is:

Message	Description
Checking Code	Handset is contacting the TFTP server to determine if it has a newer version of software that should be downloaded.
Erasing Memory	Handset has determined that a download should occur and is erasing the current software from memory. This message also displays a progress bar. When the progress bar fills the display line the erase operation is complete.
Updating Code	Handset is downloading new software into memory. The number icons at the bottom of the display indicate which file number is currently being downloaded. This message also displays a progress bar. When the progress bar fills the display line the update operation is complete on that file.

When the update is complete, the handset displays the extension number, and is ready for use.

Download Failure or Recovery Messages

The following display messages indicate a failure or recovery situation during the download process.

Message	Description
Server Busy	Handset is attempting to download from a TFTP server that is busy downloading other phones and refusing additional downloads. The handset will automatically retry the download every few seconds.
TFTP ERROR(x):yy	A failure has occurred during the TFTP download of one of the files. (x) = The file number which was being downloaded; yy is an error code describing the particular failure. Possible error codes are: 01 = TFTP server did not find the requested file. 02 = Access violation (reported from TFTP server). 07 = TFTP server reported "No such user" error. Check the TFTP server configuration. 16 = No TFTP server address. Check the TFTP server configuration. 81 = File put into memory did not CRC. The handset will attempt to download the file again. FF = Timeout error. TFTP server did not respond within a specified period of time.
Erase Failed	Download process failed to erase the memory in the handset. This operation will retry.
Waiting	Handset has attempted some operation several times and failed, and is now waiting for a period of time before attempting that operation again.

11

Troubleshooting

On occasion, you may run into transmission problems due to any number of factors originating from the wireless LAN. SpectraLink 8020/8030 Wireless Telephones can exhibit transmission problems in several ways. They can cease functioning properly, display error messages, or display incorrect data. When using and troubleshooting handsets, consider the following problem sources to determine the best method of approaching any specific situation.

Access Point Problems

Most, but not all, handset audio problems have to do with AP range, positioning, and capacity. Performing a site survey as described in this document can isolate the AP causing these types of problems. If the handset itself is suspected, conduct a parallel site survey with a handset that is known to be properly functioning.

In range/out-of-range

Service will be disrupted if a user moves outside the area covered by the wireless LAN APs. Service is restored if the user moves back within range. If a call drops because a user moves out-of-range, the handset will recover the call if the user moves back into range within a few seconds.

Capacity

In areas of heavy use, the call capacity of a particular AP may be filled. If this happens, the user will hear three chirps from the handset. The user can wait until another user terminates a call or move within range of another AP and try the call again. If a user is on a call and moves into an area where capacity is full, the system attempts to find another AP. Due to range limitations, this may be the same as moving out of range.

Transmission obstructions

Prior to system installation, the best location for APs for optimum transmission coverage should have been determined. However, small pockets of obstruction may still be present, or obstructions may be introduced into the facility after system installation. This loss of service can be restored by moving out of the obstructed area or by adding/rearranging APs.

Handset Status Messages

SpectraLink 8020/8030 Wireless Telephone status messages provide information about the SpectraLink 8020/8030 Wireless Telephone's communication with the AP and host telephone system. The following table summarizes, in alphabetical order, the status messages.

Message	Description	Action
	Download failure icon	Update handset code in the TFTP server and power cycle the handset.
3 chirps (audio)	Handset is not able to communicate with the best AP, probably because that AP has no bandwidth available.	None. This is only a warning, the call will hand off to the best AP once it becomes available.
802.1X Failure Xxxxxxxxxxxx XXX	**When WPA2-Enterprise or Cisco FSR is selected, the handset failed to connect because the user credentials are restricted based on the user account properties. In the case of EAP-FAST, the PAC ID may not match the username.** The second line of the error message contains the twelve digits of the AP MAC address and three digits that indicate the error code as defined in RFC2759.	Verify and resolve if the user account has any restrictions such password expired, account restricted/ disabled, or in case of EAP-FAST, the handset PAC and username matching the authentication server.
Address Mismatch	Handset software download files are incorrect or corrupted.	Download new software from the Polycom website per *Software Maintenance*.
Assoc Failed xxxxxxxxxxxx	x…x = AP MAC address. Handset association was refused by AP; displays MAC of failing AP.	Check handset and AP security settings. Ensure AP is configured per *VIEW Configuration Guide*. Try another AP.
Assoc Timeout xxxxxxxxxxxx	x…x = AP MAC address. Handset did not receive association response from AP; displays MAC of failing AP.	Check handset and AP security settings. Ensure AP is configured per *VIEW Configuration Guide*. Try another AP.
Auth Failed xxxxxxxxxxxx	x…x = AP MAC address. Handset authentication was refused by AP; displays MAC of failing AP.	Check handset and AP security settings. Ensure AP is configured per *VIEW Configuration Guide*. Try another AP.

Message	Description	Action
Auth Timeout xxxxxxxxxxxx	x…x = AP MAC address. Handset did not receive authentication response from AP; displays MAC of failing AP.	Check handset and AP security settings. Ensure AP is configured per *VIEW Configuration Guide*. Try another AP.
Bad Code Type xx Expected Code Type yy	xx, yy = software license types. Handset software does not match current handset license selection.	Download new software from the Polycom website per *Software Maintenance*.
Bad Config	Some needed configuration parameter has not been set.	Check all required handset configuration parameters for valid settings.
Bad SSID	The handset has not had an SSID entered.	Statically configure an SSID in the **Admin** menu.
Bad Phintl File	Handset software download files are incorrect or corrupted.	Download new software from the Polycom website per *Software Maintenance*.
Bad Program File	Handset software download files are incorrect or corrupted.	Download new software from the Polycom website per *Software Maintenance*.
Bad SIP TFTP IP	A bad unicast address has been entered for the SIP TFTP server in static entry mode.	Re-enter the correct IP address in the administrative menus for static IP addresses.
(battery icon), Battery Low, beep (audio)	Low battery.	In call: the battery icon displays and a soft beep will be heard when the user is on the handset and the battery charge is low. User has 15–30 minutes of battery life left. Not in call: The battery icon displays whenever the battery charge is low The message Battery Low and a beep indicate a critically low battery charge when user is not on the handset. The handset will not work until the Battery Pack is charged.
Battery Failure	The Battery Pack is not functioning.	Replace the Battery Pack with a new or confirmed SpectraLink Battery Pack. Only SpectraLink Battery Packs will work.
Battery Failed	Battery Pack is damaged or incompatible with handset.	Replace the Battery Pack with a new or confirmed SpectraLink Battery Pack. Only SpectraLink Battery Packs will work.
Can't Renew DHCP yyy.yyy.yyy.yyy	y…y = DHCP server IP address. DHCP server is not responding to initial renewal attempt.	Configuration problem. Check the IP address configuration in the DHCP server.

Message	Description	Action
Cert Expired	When WPA2-Enterprise with PEAP authentication is selected, the handset failed to connect due to an expired certificate on the handset or authentication server.	Verify that the NTP server is properly configured with the correct time. Verify that the certificates loaded on the handset and authentication server have valid start/end dates by looking at "valid to" field from "validity" data in certificates. If any of the certificates have expired replace them with new certificates.
Cert Invalid	When WPA2-Enterprise with PEAP authentication is selected, the Wireless Telephone failed to connect to the network because the certificate start date is in the future.	Verify that the NTP server is properly configured with the correct time. Verify that the certificates loaded on the handset and authentication server have valid start/end dates by looking at "valid from" field from "validity" data in certificates. If any of the certificates have expired replace them with new certificates.
Charging …	The handset is charging in the desktop charger.	No action needed.
Charge Complete	The handset is now fully charged.	No action needed.
Charger Error	The handset has detected a problem with the charging circuitry.	Allow the charger and battery to cool. If the problem persists, try a new or confirmed battery. If the problem still persists, contact technical support and report the error.
Checking Code	Handset is contacting the TFTP server to determine if it has a newer version of software that should be downloaded.	None, this message should only last for approximately one second. If message remains displayed, power off and contact customer support for a replacement phone.
Checking DHCP IP	The handset is retrieving DHCP information from the DHCP server.	None. This is informational only.
CRC Code Error	The software which has been TFTP downloaded has a bad redundancy code check.	Try the download again; it is possible the software was corrupted during download. If the error repeats, check that the download image on the TFTP server is not corrupted.
Code Mismatch!	The software loaded into the handset is incorrect for this model handset.	Verify the License Management value is correct. Replace the software image on the TFTP server with software that is correct for the handset model.
DCA Timeout	The handset has detected a fault for which it cannot recover, possibly due to a failure to acquire any network.	Turn the handset off, then on again. If error persists, contact Polycom Technical Support and report the error.
DHCP Error (1-5)	DHCP Error 1.	The handset cannot locate a DHCP server. It will try every four seconds until a server is located.

Message	Description	Action
	DHCP Error 2.	The handset has not received a response from the server for a request to an IP address. It will retry until a server is found.
	DHCP Error 3.	The server refuses to lease the handset an IP address. It will keep trying.
	DHCP Error 4.	The server offered the handset a lease that is too short. The minimum lease time is 10 minutes but Polycom Engineers recommend at least one-hour minimum lease time. The handset will stop trying. Reconfigure the server and power cycle the handset.
	DHCP Error 5.	Failure during WEP Key rotation process (proprietary feature).
DHCP Lease Exp yyy.yyy.yyy.yyy	y…y = DHCP server IP address. DHCP is not responding to renewal attempts (at least one renewal succeeded).	The handset failed to renew its DHCP lease, either because the DHCP server is not running, or because the configuration has been changed by the administrator. The handset will attempt to negotiate a new lease, which will either work, or it will change to one of the above DHCP errors (1 through 4).
DHCP NACK error yyy.yyy.yyy.yyy	y…y = DHCP server IP address. DHCP server explicitly refused renewal.	The DHCP lease currently in use by the handset is no longer valid, which forces the handset to restart. This problem should resolve itself on the restart. If it does not, the problem is in the DHCP server.
DL Not On Sector	Handset software download files are incorrect or corrupted.	Download new software from the Polycom website per *Software Maintenance*.
DO NOT POWER OFF	The handset is in a critical section of the software update.	None. Do not remove the Battery Pack or attempt to power off the phone while this is displayed. Doing so may require the handset inoperable.
Duplicate IP	The handset has detected another device with its same IP address.	If using DHCP, check that the DHCP server is properly configured to avoid duplicate addresses. If using Static IP, check that the handset was assigned a unique address.
Erase Failed	Download process failed to erase the memory in the handset.	Operation will retry but may eventually report the error "int. error: 0F" Power cycle the handset.

Message	Description	Action
Erasing Memory	Handset has determined that a download should occur and is erasing the current software from memory.	None. When the progress bar fills the display line the erase operation is complete. Do not turn the handset off during this operation.
Files Too Big	Handset software download files are incorrect or corrupted.	Download new software from the Polycom website per *Software Maintenance*.
Flash Config Error	Handset internal configuration is corrupt.	Perform "Restore Defaults" operation via administrator menus (or re-program with Configuration Cradle).
Initializing …	The handset is performing power-on initialization.	None. This is informational only.
Initializing SIP	The handset is performing a power-on initialization of the SIP application. The phone is initializing its data structures and attempting to access the SIP TFTP server and download the SIP configuration files.	None. This is informational only.
Internal Err. # #	The handset has detected a fault from which it cannot recover.	Record the error code so it can be reported. Turn the handset off then on again. If error persists, try registering a different handset to this telephone port. If error still persists, contact Polycom Technical Support and report the error.
Invalid Usr/Pwd	When WPA2-Enterprise or Cisco FSR is selected, the handset failed to connect due to incorrect device credentials or unavailability of authentication server. If the error is because of the incorrect device credentials then the username or password doesn't match with those configured on the authentication server.	Verify that the required credentials {username, password} are created on the authentication server and should match the handset. This may also happen when the authentication server is not reachable while doing the EAP authentication. Make sure the authentication server is active and reachable from the WLAN access points/controller at all times.
Multiple GW Res	More than one SpectraLink 8000 SVP Server has responded.	Caused by two or more handsets sharing the same IP address. Assign unique IP addresses to each handset.
Multiple SVP Reg yyy.yyy.yyy.yyy	y…y = SVP IP address Handset received responses from multiple SVP Servers; displays IP address of one responding SVP Server.	This can happen if the handset has been reconfigured to use a different SVP server and then powered on before the previous server has had time to determine that the handset is no longer connected to it. The problem should go away after about 30 seconds.

Message	Description	Action
Must Upgrade SW!	Handset software is incompatible with hardware.	Download new software from the Polycom website per *Software Maintenance*.
Net Busy xxxxxxxxxxxx	x…x = AP MAC address. Handset cannot obtain sufficient bandwidth to support a call; displays MAC of failing AP.	Try the call again later.
No 802.11a Sub-bands Enabled	'a' radio selected but no sub-bands are enabled	Configure 'a' radio sub-bands from **Admin** menus
No 802.11 Sub-bands Enabled	'b/g radio selected but no sub-bands are enabled	Configure 'b/g' radio sub-bands from **Admin** menus
No APs Heard	The handset is unable to hear beacons/probes from any AP in the network in site survey mode.	Verify that network is properly configured and the handset is able to hear beacons from the AP.
No DHCP Server	Handset is unable to contact the DHCP server.	Check that DHCP is operational and connected to WLAN or use Static IP configuration in the handset.
No ESSID	Attempted to run Site Survey application without an ESSID set.	Let handset come completely up. Statically configure an ESSID in the **Admin** menu.
No Func Code	Handset software download files are incorrect or corrupted.	Reconfigure the handset to gain access to the WLAN and download new code.
No Host IP	The handset is configured for “static IP” (as opposed to “use DHCP”) and no valid host IP address (the handset’s IP address) has been entered.	Enter a valid IP address in the configuration settings or change to “use DHCP.”
No IP Address	Invalid IP.	Check the IP address of the handset and reconfigure if required.
No Net Access	Cannot authenticate / associate with AP.	Verify the AP configuration. Verify that all the WEP settings in the handset match those in the APs.
No Net Found No APs	This indicates that the handset cannot find any access points and has no additional information to display as to why. Possible problems are enumerated below.	
	No radio link.	Verify that the AP is turned on.
	No ESSID: Auto-learn not supported (or) incorrect ESSID.	Verify the ESSID of the wireless LAN and enter or Autolearn it again if required.
	AP does not support appropriate data rates.	Check the AP configuration against Configuration Guide for AP.
	Out of range.	Try getting closer to an AP. Check to see if other handsets are working within the same range of an AP. If so, check the ESSID of this handset.

Message	Description	Action
	Incorrect Security settings.	Verify that all the Security settings in the handset match those in the APs.
No Net Found xxxxxxxxxxxx yy	x…x = AP MAC address. yy = AP signal strength. Handset cannot find a suitable AP; displays MAC and signal strength of "best" non-suitable AP found.	Check AP and handset network settings such as ESSID, Security, Reg domain and Tx power. Ensure APs are configured per *Configuration Guide*. Try Site Survey mode to determine a more specific cause.
No Net Found No CCX APs	The Wireless Telephone is configured for CCX compatible operation, but cannot find an access point that is advertising CCX capability.	Check the AP configuration against *VIEW Configuration Guide* for AP.
No Net Found No CCKM APs	The Wireless Telephone is configured to use CCKM for fast and secure handoffs, but cannot find an access point that is configured appropriately.	Check the AP configuration against *VIEW Configuration Guide* for AP.
No Net Found No WMM APs	The Wireless Telephone is configured to use Wi-Fi Standard QoS, but cannot find an AP configured appropriately.	Check the AP configuration against *VIEW Configuration Guide*.
No PBX Response	The handset has exceeded its retransmission limit with no ACK response from proxy server.	Verify that proxy server IP address and port are properly configured.
No Reg Domain	Regulatory Domain Not Set.	Configure the Regulatory Domain of the handset.
No Server IP	In the case of static IP configuration, the handset failed to find the call server IP.	Verify that call server info is properly configured on the handset.
No SIP TFTP IP	No IP address has been entered for the SIP TFTP server.	In static IP mode the SIP TFTP server address must be entered in the administrative menus.
No SIP user file	The phone is attempting to download a SIP configuration file from the SIP TFTP server. A file must be available for the username that was entered either in the **Admin** menus or as requested at power-on.	Ensure a SIP configuration file is available on the SIP TFTP server and is named as specified (sip_username.cfg).
No SVP IP	The handset is configured for "Static IP" (as opposed to "use DHCP"), and no valid SpectraLink 8000 SVP Server address has been entered.	Enter a valid SpectraLink 8000 SVP Server IP address in the configuration setting or change to "use DHCP."

Message	Description	Action
No SVP Response yyy.yyy.yyy.yyy	y…y = SVP Server IP address. Handset has lost contact with the SVP Server.	This may be caused by bad radio reception or a problem with the SpectraLink 8000 SVP Server. The handset will keep trying to fix the problem for 20 seconds, and the message may clear by itself. If it does not, the handset will restart. Report this problem to the system administrator if it keeps happening.
No SVP Server	Handset can't locate SpectraLink 8000 SVP Server. SpectraLink 8000 SVP Server is not working. No LAN connection at the SpectraLink 8000 SVP Server.	IP address configuration of SpectraLink 8000 SVP Server is wrong or missing. Check error status screen on SpectraLink 8000 SVP Server. Verify SpectraLink 8000 SVP Server connection to LAN.
No SVP Server No DNS Entry	Handset unable to perform DNS lookup for SVP Server, server had no entry for SVP Server.	The network administrator must verify that a proper IP address has been entered for the SVP Server DHCP option 151.
No SVP Server No DNS IP	Handset unable to perform DNS lookup for SVP Server, no IP address for DNS server.	The network administrator must verify proper DHCP server operation.
No SW Found	A required software component has not been identified.	Check that the handset license type has a corresponding entry in the slnk_cfg.cfg file. Check that the pd11sid.bin and pi110000.bin entries exist in under this license type in the slnk.cfg.cfg file.
No TFTP Response	The handset could not get the TFTP server to respond.	The handset will continue to boot without checking if its current code is the latest available. Check that the TFTP server is operational. If the Wireless Telephone is using DHCP, check that the DHCP options are set correctly.
No WPA PassPhrase	This error only appears when the Admin Menus are exited. The handset is configured for WPA-PSK or WPA2-PSK and no pass phrase or shared key has been entered.	Enter the pass phrase or pre-shared key and restart the handset
Not Installed!	A required software component is missing.	Check that all required software files are on the TFTP server, if over-the-air downloading is being used. If the error repeats, contact Polycom Technical Support.
Press END	The far end of a call has hung up.	Hang up the near end.

Message	Description	Action
Press END to quit	The handset is waiting to acquire bandwidth required for voice communication.	Press **END** or wait until bandwidth is available.
Prom Bad Length	The handset software downloaded files that are incorrect or corrupted.	Download new software from the OEM site per *Software Maintenance*.
Registering	The handset has completed initialization of the SIP application and is attempting to register lines to the SIP proxy servers.	If registrations are failing, the phone can stay in this state for a considerable length of time. After the phone leaves this state, press the **LINE** key to view what lines have failed to register. Ensure usernames and passwords have been entered in administrative menus for registrations that have failed and that proxy information is correct in the SIP configuration files.
RTP Open Failed	The handset attempted to open an RTP port for audio but was unsuccessful.	Verify that SpectraLink 8000 SVP Server capacity has not been exceeded.
Select License	The correct protocol has not been selected from the license set.	Using the **Admin** menu, select one license from the set to allow the phone to download the appropriate software.
Server Busy	Handset is attempting to download from a TFTP server that is busy downloading other devices and refusing additional downloads.	None, the handset will automatically retry the download every few seconds.
SIP Login	Prompt for login information – username and password.	At power-on initialization, no username was detected in the **Admin** menu items for SIP registrations. Enter a valid username and password for an existing SIP configuration file.
Skt Open Fail	Socket open fail. Occurs when the handset attempts to open a connection to the proxy server but fails.	Verify that SpectraLink 8000 SVP Server capacity has not been exceeded.
Service Rej.	The SpectraLink 8000 SVP Server has rejected a request from the handset.	The handset will restart and attempt to re-register with the SpectraLink 8000 SVP Server, which should fix the problem. Report to your administrator if it keeps happening.
Storing Config	Handset is storing changes to handset configuration.	None. Informational only. The handset may display this briefly following a configuration change or software download.
SVP Service Rej.	The SpectraLink 8000 SVP Server has rejected a request from the handset.	The handset will restart and attempt to re-register with the SVP Server, which should fix the problem. Report to your administrator if it keeps happening.

Message	Description	Action
System Busy yyy.yyy.yyy.yyy	y…y = SVP Server IP Address. SVP Server has reached call capacity.	All call paths are in use, try the call again in a few minutes.
System Locked (with Busy Tone)	SpectraLink 8000 SVP Server is locked.	Try call again later, system has been locked for maintenance.
TFTP ERROR(x):yy	A failure has occurred during a TFTP software download. (x) = The file number which was being downloaded; yy is an error code describing the particular failure. Possible error codes are: 01 = TFTP server did not find the requested file. 02 = Access violation (reported from TFTP server). 07 = TFTP server reported "No such user" error. 16 = No TFTP server address. 81 = File put into memory did not CRC. FF = Timeout error. TFTP server did not respond within a specified period of time.	Error code 01, 02, 07, or 16 - check the TFTP server configuration. Error code 81, the handset will attempt to download the file again. For other messages, power off the handset, then turn it on again to retry the download. If the error repeats, note it and contact Polycom Customer Support.
Too Many Errors	The handset continues to reset and cannot be recovered.	Fatal error. Return handset to Polycom.
Unknown xx:yy:zz	A phrase is missing from the phintl file.	Download new software from the Polycom website per *Software Maintenance*.
Updating …	The handset is internally updating its software images.	None. The handset may do this briefly after a download. This is informational only.
Updating Code…	Handset is downloading new software into memory. The number icons at the bottom of the display indicate which file number is currently being downloaded. This message also displays a progress bar. When the progress bar fills the display line the update operation is complete on that file.	None. When the progress bar fills the display line the update operation is complete on that file. Do not turn the handset off during this operation.
Wait for bandwidth	The phone is waiting for bandwidth sufficient for voice communication.	No action required. You will have the option of pressing **END** to abort the phone call.
Waiting…	Handset has attempted some operation several times and failed.	None. The handset is waiting for a specified period of time before attempting that operation again.
Wrong Code Type	The software loaded into the handset is incorrect for this model phone.	Replace the software image on the TFTP server with software that is correct for the handset model.

Appendix A: Regulatory Domains

This table details the specifications for regulatory domain settings. Polycom recommends that you check with local authorities for the latest status of their national regulations for both 2.4 and 5 GHz wireless LANs.

Domain Identifier	802.11 Mode	Band	Channels	DFS Required?	Max. Power Limit (peak power)	Countries
01	g only b & b/g mixed		1 – 11	n/a	100mW (+20dBm)	US Canada Brazil
	a	5.1500 – 5.2500 GHz	36 – 48	No	50mW (+17dBm)	
		5.2500 – 5.3500 GHz	52 – 64	Yes	100mW (+20dBm)	
		5.4700 – 5.7250 GHz	100 – 140	Yes		
		5.7250 – 5.8250 GHz	149 – 161	No		
02	g only b & b/g mixed		1 – 13	n/a	100mW (+20dBm)	Europe Australia New Zealand
	a	5.1500 – 5.2500 GHz	36 – 48	No		
		5.2500 – 5.3500 GHz	52 – 64	Yes		
		5.4700 – 5.7250 GHz	100 – 140	Yes		
03	g only b & b/g mixed		1 – 13	n/a	100mW (+20dBm)	Japan
	a	5.1500 – 5.2500 GHz	36 – 48	No		
		5.2500 – 5.3500 GHz	52 – 64	Yes		
04	g only b & b/g mixed		1 – 13	n/a	100mW (+20dBm)	Singapore
	a	5.1500 – 5.2500 GHz	36 – 48	No		
		5.2500 – 5.3500 GHz	52 – 64	Yes		
05	g only b & b/g mixed		1 – 13	n/a	100mW (+20dBm)	Korea
	a	5.1500 – 5.2500 GHz	36 – 48	No		
		5.2500 – 5.3500 GHz	52 – 64	Yes		
		5.4700 – 5.6500 GHz	100 – 124	Yes		
		5.7250 – 5.8250 GHz	149 – 161	No		

Domain Identifier	802.11 Mode	Band	Channels	DFS Required?	Max. Power Limit (peak power)	Countries
06	g only b & b/g mixed		1 – 11	n/a	100mW (+20dBm)	Taiwan
	a	5.2500 – 5.3500 GHz	52 – 64	Yes		
		5.4700 – 5.7250 GHz	100 – 140	Yes		
		5.7250 – 5.8500 GHz	149 – 165†	No		
07	g only b & b/g mixed		1 – 13	n/a	100mW (+20dBm)	Hong Kong
	a	5.1500 – 5.2500 GHz	36 – 48	No	50mW (+17dBm)	
		5.2500 – 5.3500 GHz	52 – 64	Yes	100mW (+20dBm)	
		5.4700 – 5.7250 GHz	100 – 140	Yes		
		5.7250 – 5.8250 GHz	149 – 161	No		
08	g only b & b/g mixed		1 – 11	n/a	100mW (+20dBm)	Mexico India
	a	5.1500 – 5.2500 GHz	36 – 48	No		
		5.2500 – 5.3500 GHz	52 – 64	Yes		
		5.7250 – 5.8500 GHz	149 – 161	No		

† Channel 165 is not currently supported on the handset when the UNI-3 (5.7250 – 5.8250) band is enabled for 802.11a.

Index

A

Access point
- Coverage 106
- Coverage test 117

Access point, description 15

C

Capacity 123
Checking code 122
Customer Support Hotline 4

D

Download messages
- Failure or Recover 122
- Normal 122

E

Erasing memory 122
Ethernet Switch, description 16

H

Hotline 4

O

OAI
- OAI Gateway 34
- OAI On/Off 34
- OAI Server IP 34, 38

Obstructions 124
Out of range 123

R

Regulatory Domain 41
Restore Defaults 44, 45

S

Site Certification 117
Status messages 125

T

Transmission obstructions 124

U

Updating code 122

W

Wireless Telephone
- Problems with 123
- Status messages 125

WT, description 15